Адміністративне право і процес

УДК 341:004+342.9

Тарасюк Анатолій Васильович
кандидат юридичних наук, головний науковий співробітник
Наукової лабораторії забезпечення інформаційної
та кібернетичної безпеки
НДІ інформатики і права НАПрН України
Тарасюк Анатолий Васильевич
кандидат юридических наук, главный научный сотрудник
Научной лаборатории обеспечения информационной
и кибернетической безопасности
НИИ информатики и права НАПрН Украины
Tarasyuk Anatoliy
Candidate of Law, Chief Scientist of the
Scientific Laboratory for Information and Cyber Security
Research Institute of Informatics and Law of the
National Academy of Science of Ukraine
ORCID: 0000-0002-0479-0666

ПРІОРИТЕТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ДОСВІД ОКРЕМИХ КРАЇН
ПРИОРИТЕТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ: ОПЫТ ОТДЕЛЬНЫХ СТРАН
CYBERSECURITY PRIORITIES: COUNTRY EXPERIENCE

Анотація. *Розглянуто загальні політичні та економічні чинники актуалізації проблем кібербезпеки на національному, наднаціональному та глобальному рівнях. Зроблено висновок, що відмінною рисою німецького підходу до забезпечення кібербезпеки є його комплексний і*

фундаментальний характер, який включає цілу систему нормативних актів, планів і інститутів. Виявлено основні підходи й тенденції, пов'язані з виробленням на наднаціональному рівні ЄС єдиної стратегії в області кібербезпеки. Встановлено, що основна проблема ефективного забезпечення кібербезпеки полягає у створенні в ЄС єдиного європейського політичного простору. Значна активність в цій сфері керівних органів ЄС стикається з нездатністю ряду країн в повному обсязі виконати всі директиви, розпорядження, регламенти та інші нормативні акти. Через складні процедури узгодження на національному і наднаціональному рівнях, що вимагає значного часу, а також через несформованість в ЄС єдиного політичного простору, держави і наднаціональні структури ЄС не завжди встигають вчасно реагувати на появу нових кіберзагроз. Проте, не дивлячись на ці проблеми, система забезпечення кібербезпеки в країнах ЄС досить швидко розвивається і вдосконалюється, чому сприяє настільки ж швидке накопичення досвіду регулювання і координації дій країн - членів ЄС у сфері кібербезпеки. За результатами дослідження визначено, що в умовах розробки нашою державою національного законодавства у сфері кібернетичної безпеки (з урахування умов Угоди про асоціацію між Україною та ЄС) для України за умови відповідного корегування може бути корисним досвід ЄС щодо визначення або створення єдиного державного органу з питань кіберзахисту, здатного відповідати на кібератаки, сертифікація цифрових продуктів і послуг, заходи із захисту персональних даних користувачів комп'ютерних мереж, що передбачають значні штрафи за незаконне використання цих даних.

Ключові слова: *кібербезпека, ЄС, загрози, кіберпростір, інформація, дані.*

Аннотация. *Рассмотрены общие политические и экономические факторы актуализации проблем кибербезопасности на национальном,*

наднациональном и глобальном уровнях. Сделан вывод, что отличительной чертой немецкого подхода к обеспечению кибербезопасности является его комплексный и фундаментальный характер, включающий целую систему нормативных актов, планов и институтов. Выявлены основные подходы и тенденции, связанные с выработкой на наднациональном уровне ЕС единой стратегии в области кибербезопасности. Установлено, что основная проблема эффективного обеспечения кибербезопасности заключается в создании в ЕС единого европейского политического пространства. Значительная активность в этой сфере руководящих органов ЕС сталкивается с неспособностью ряда стран в полном объеме выполнить все директивы, распоряжения, регламенты и другие нормативные акты. Через процедуры согласования на национальном и наднациональном уровнях, требует значительного времени, а также из-за несформированности в ЕС единого политического пространства, государства и наднациональные структуры ЕС не всегда успевают своевременно реагировать на появление новых киберугроз. Однако, несмотря на эти проблемы, система обеспечения кибербезопасности в странах ЕС достаточно быстро развивается и совершенствуется, чему способствует столь же быстрое накопление опыта регулирования и координации действий стран - членов ЕС в сфере кибербезопасности. По результатам исследования установлено, что в условиях разработки нашим государством национального законодательства в сфере кибернетической безопасности (с учетом условий Соглашения об ассоциации между Украиной и ЕС) для Украины при условии соответствующей корректировки может быть полезным опыт ЕС по определению или создание единого государственного органа по вопросам киберзащиты , способного отвечать на кибератаки, сертификация цифровых продуктов и услуг, меры по защите персональных данных пользователей компьютерных сетей, предусматривающие значительные штрафы за

незаконное вы вания этих данных.

Ключевые слова: *кибербезопасность, ЕС, угрозы, киберпространство, информация, данные.*

Summary. *The aim of the article is to analyze the most complex and urgent problems of cybersecurity in EU countries and to formulate a common policy in this area. Common political and economic factors for cybersecurity issues at national, supranational and global levels are considered. It is concluded that the hallmark of the German approach to cybersecurity is its complex and fundamental character, which includes a whole system of regulations, plans and institutions. The main approaches and trends related to the development of a unified EU cyber security strategy have been identified. It is established that the main problem of effective cyber security is to create a single European political space in the EU. Significant activity in this area of EU governing bodies is faced with the inability of a number of countries to fully comply with all directives, regulations, regulations and other regulations. Due to complex coordination procedures at the national and supranational levels, which require considerable time, as well as the lack of a single political space in the EU, EU states and supranational structures do not always have time to respond to the emergence of new cyber threats. However, in spite of these problems, the cybersecurity system in the EU countries is developing and improving quite rapidly, which contributes to the equally rapid accumulation of experience in regulating and coordinating EU member states in the field of cybersecurity. According to the results of the study, it is determined that in the conditions of our country's development of national legislation in the field of cyber security (taking into account the terms of the Association Agreement between Ukraine and the EU) for Ukraine, provided appropriate adjustment, it may be useful for the EU experience to identify or create a single state body for cyber defense capable of responding to cyberattacks, certification of digital products and services, measures to protect the personal data of users of computer*

networks, which entail significant penalties for illegal use of this data.

Keywords: *cybersecurity, EU, threats, cyberspace, information, data.*

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Відсутність в Україні достатнього законодавчого забезпечення кібербезпеки в умовах гібридної війни значно підвищує ризики руйнування національної системи кібербезпеки, розвитку деструктивних впливів на національну безпеку, а також підривається впевненість в українській складовій забезпечення європейської та світової кібербезпеки. Національний координаційний центр кібербезпеки, який є робочим органом РНБО України, на сьогодні позбавлений можливості повномасштабно та системно здійснювати координацію щодо законодавчого та нормативно-правового забезпечення ефективної системи кібербезпеки в Україні, в основі якої лежав би комплексний аналіз ситуації у цій галузі, викликів, існуючих та імовірних небезпек і врахування інтересів кожного учасника та суб’єкта і яка б інтегрувалася до європейської та глобальної міжнародних систем кібербезпеки, мала б достатню фінансову, організаційну, технічну, кадрову підтримку. У зв’язку з цим необхідно вивчати зарубіжний досвід, створюючи в нашій країні ефективну систему, за якою забезпечуватиметься правовий та організаційний аспекти кібернетичної безпеки, імплементації окремих аспектів у національну практику, а також розширення співпраці в досліджуваній сфері.

Аналіз останніх досліджень і публікацій. Питання забезпечення кібернетичної безпеки, в тому числі в контексті вивчення зарубіжного досвіду, були предметом наукової уваги багатьох вчених. Серед наукових праць, які слугували теоретичними орієнтирами для данаої статті доцільно виокремити наступних дослідників М. Камчатного [1], Р. Гейні [6], В. Пантіна [7], М. Гребенюка та Б. Леонова [15]. Водночас, досвід

забезпечення кібербезпеки у зарубіжних країнах, передусім з точки зору можливостей його використання у вітчизняних реаліях, лишається дослідженим недостатньо.

Формулювання цілей статті (постановка завдання). Проаналізувати найбільш складні та актуальні проблеми забезпечення кібербезпеки у зарубіжних країнах та формування державної політики у цій сфері.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Відповідно до зростаючої ролі кіберпростору багато держав створюють власні національні законодавчі норми та стратегії кібербезпеки. Так, нині 27 країн-членів НАТО, Європейський Союз (ЄС), 12 країн Європи, що не є членами НАТО, а також 38 країн із інших частин світу мають власні національні стратегії кібербезпеки [1].

Ухвалена Стратегія кібербезпеки Європейського Союзу 2013 року – це перший всеохоплюючий документ системного характеру у цій галузі. В ньому охоплено кожен аспект кібернетичного простору: внутрішній ринок, правосуддя, внутрішня та зовнішня політика.

Окрім Стратегії, відбулася розробка та ухвалення законодавчої пропозиції посилити безпеку інформаційних систем Євросоюзу.

Міжнародна політика Європейського Союзу щодо кіберпростору має ряд визначених Стратегією пріоритетних напрямів, серед яких доцільно виокремити наступні:

– засади свободи та відкритості: стратегією визначаються принципи, за якими реалізуються основоположні людські та громадянські права у кіберсередовищі;
– використання законодавчої бази Європейського Союзу у кібернетичному просторі аналогічно до фізичного світу. Що важливо в даному аспекті, це той принципово важливий підхід, відповідно до

якого відповідальним за безпеку цього простору є як пересічні громадяни, так і держави загалом;

– потенціал кібернетичної безпеки повинен розвиватися за допомогою співробітництва та партнерства, до якого залучені міжнародні партнери та організації, приватний сектор та громадянське суспільство [2].

З визначених напрямів випливає один суттєвий висновок: кібербезпека є справою всіх: самої людини, приватного сектора, суспільства і держави. Тільки у рамках цього симбіозу вбачається можливість побудови суспільства у якому індивіди будуть почувати себе безпечно у кіберпросторі. Досягнути цього можливо за умови ряду складових:

1) тісної співпраці держави, в особі відповідальних за кібербезпеку органів, та приватного сектору і громадян. Така співпраця першочергово полягає у взаємному обміні інформацією;

2) розвиток та практичне втілення таких категорій як «екологія інформації», «інформаційна гігієна», «критичне мислення у споживачів інформації», розвиток інформаційної культури, а також усвідомлення необхідності навчання дітей та молоді інформаційній культурі та гігієні.

Водночас, слід враховувати, що країни ЄС різняться за рівнем соціально-економічного і технологічного розвитку, рівнем розвитку цифрової економіки та масштабами використання Інтернету. У зв'язку з цим в цілому ряді країн ЄС національна стратегія з кібербезпеки або розроблена в недостатній мірі, не зважаючи на вимоги Європейської комісії.

Виходячи з показників глобального рейтингу кібербезпеки (враховує показники країни у п'яти сферах: правові норми в області кібербезпеки і їх виконання; технічні заходи і наявність відповідних інструментів для їх реалізації; організаційні заходи в сфері кібербезпеки; розвиток потенціалу кібербезпеки; участь у міжнародному співробітництві щодо її забезпечення [3, с. 39]), найбільш передовими в галузі розробки і застосування

національних стратегій кібербезпеки серед країн - членів ЄС є Норвегія, Естонія, ФРН, Австрія, Угорщина, Нідерланди [3, с. 14]. Найменш успішними в плані кібербезпеки серед країн, що входять в ЄС, є Румунія, Болгарія, Бельгія, Португалія, Греція [3, с. 15].

У Нідерландах, як вважає асоціація виробників програмного забезпечення BSA [4], найрозвиненіша та найбільш "зріла" система кібернетичної безпеки, як з погляду правової підтримки, так і з погляду технологій та організації. Ця країна через кожні два роки здійснює перегляд своєї Національної Стратегії кібербезпеки, а Національним Центром кібербезпеки, який є національним CERT (англ. ***c****omputer* ***e****mergency* ***r****esponse* ***t****eam*, CERT) з рядом додаткових повноважень, здійснюється розробка та запровадження усіх процедурних та технологічних питань стосовно безпеки в кіберпросторі. Цим же Центром проводиться активна співпраця з Аналітичними та інформаційними центрами (ISACs), які дбають про те, щоб критична інформаційна інфраструктура за секторами була у безпеці.

Створення "Гарячої лінії" meldpunt-kinderporno.nl ініціював голландський Інтернет-провайдер для протидії дитячій порнографії як приватна структура, проте зрештою цю ініціативу підтримало Міністерство юстиції Нідерландів.

До слова, саме Нідерланди були ініціаторами створення загальноєвропейських мереж "гарячих ліній" – InHope [5] і перші впровадили у своїй національній практиці.

Якщо вести мову про організацію забезпечення кібербезпеки в країнах Європи в цілому, слід зауважити, що у 2013 р. була представлена стратегія кібербезпеки ЄС під назвою «Відкритий, безпечний і надійний кіберпростір». Метою цієї стратегії є підвищення стійкості та нарощування потенціалу в області кібербезпеки держав - членів ЄС, включаючи посилення боротьби з кіберзлочинністю, формування ефективної інфраструктури забезпечення інформаційної безпеки, розробку принципів

координації міжнародної політики в області кібербезпеки. Серед інших значущих актів, спрямованих на формування єдиної політики ЄС з протидії кіберзагрозам, слід відзначити «Директиву ЄС з кібербезпеки» [6]. Відповідно до цієї директиви, держави-члени ЄС спільно з Європейською Комісією та Європейським агентством з мережевої та інформаційної безпеки (ENISA) повинні створити групу взаємодії. Основними функціями цієї групи є обмін інформацією між її учасниками, а також боротьба із загрозами і інцидентами у сфері кібербезпеки. Крім того, в директиві міститься вимога створити мережу національних груп з метою організації швидкої і ефективної операційної взаємодії й підтримки країн - членів ЄС для вирішення транскордонних інцидентів в кіберпросторі. Ця директива, розроблена Європейською комісією і схвалена Європарламентом, набула чинності в серпні 2016 р. З цього моменту почався процес імплементації основних положень директиви в національному законодавстві країн - членів ЄС і визначення операторів, які будуть на практиці забезпечувати кібербезпеки в Європі.

Ще одним заходом, покликаним посилити кібербезпеку ЄС, стало запропоноване Європейською комісією в 2017 р. введення сертифікатів для цифрової продукції і цифрових послуг, що випускаються в країнах ЄС. З точки зору Єврокомісії, сертифікація може відігравати вирішальну роль в посиленні безпеки і розвитку єдиного європейського ринку цифрових продуктів і послуг, оскільки сертифікати будуть дійсними на всій території ЄС і зможуть гарантувати відповідність продуктів і послуг вимогам кібербезпеки [7, с. 11].

Важливим кроком на шляху захисту даних користувачів комп'ютерних мереж також став загальний регламент ЄС про захист даних (General Data Protection Regulation, GDPR), розроблений і схвалений Європейським парламентом ще в 2016 р. і набрав чинності у травні 2018 р. Цей регламент, покликаний регулювати поширення та використання

особистих даних громадян країн ЄС, встановлює норми, відповідно до яких користувачі з країн ЄС мають право знати, як саме використовуються їхні персональні дані, які вони надають про себе в комп'ютерних мережах. Нові правила є екстериторіальними і поширюються на операторів, які обробляють персональні дані європейців не тільки в країнах ЄС, а й за його межами [7, с. 14].

Досить прогресивним кроком ЄС на шляху забезпечення кібербезпеки стало створення на початку березня 2020 року, з ініціативи Литви, кібернетичних сил Євросоюзу швидкого реагування (Cyber Rapid Response Team, CRRT [8]), до складу яких увійшли представники шести європейських держав (Литва, Естонія, Хорватія, Польща, Нідерланди та Румунія). Це було остаточно погоджено 4 березня в Загребі (Хорватія) у Меморандумі про взаєморозуміння. Документ юридично дозволяє роботу таких груп у юрисдикціях різних країн, визначає механізм роботи CRRT, правовий статус, ролі і процедури. Створені цивільними і військовими експертами, CRRT приєднаються до нейтралізації і розслідування небезпечних кіберінцидентів практично або, за необхідності, фізично [9]. Статус спостерігача у даному об’єднанні отримали Бельгія, Греція, Іспанія, Італія, Франція, Словенія і Фінляндія.

Розвідслужби Литви у 2019 році оголосили, що в кіберпросторі Литви простежується шкідницька діяльність кібернетичних потужностей Росії і Китаю. У традиційній оцінці загроз нацбезпеці зазначається, що найбільшу загрозу для безпеки інформаційних систем і інформації, що зберігається в них, є кібершпіонаж розвідслужб Росії, а новим фактором ризику може стати розвиток технологій 5G, якщо не буде приділятися належна увага надійності постачальника послуг або продуктів інформаційних технологій [10].

Позитивними прикладами для України можуть слугувати практичні знання, яких набула Естонія, єдина пострадянська держава, що має значні успіхи у створенні системи кібернетичного захисту.

2007 року Естонії випало бути першою країною-членом НАТО, кіберпростір якої було атаковано хакерами, і цей напад підтримувала інша держава. Захист держави в кіберсередовищі здійснювався громадянами – кваліфікованими ІТ-інженерами, які разом обміркували і взялися до впровадження системи захисту. Естонцями було створено такі стандарти кібернетичної безпеки, які пізніше перейняло НАТО задля впровадження у власному оборонному та безпековому сегменті. Зараз у світ є 32 центри, які користуються саме естонськими стандартами. На цей час в державі, яка має населення 1,2 мільйони людей, функціонує 5 кібернетичних центрів. Актуальність естонського досвіду для України пов'язана з багатьма аспектами: спільним минулим, територіальною близькістю, однаковими зовнішніми чинниками, які викликали в Естонії потребу оперативного створення системи кібернетичного захисту.

Країни Балтії, які чітко усвідомили потенційний вплив від ескалації конфлікту в Україні на їхню безпеку. Передусім це Польща та країни Прибалтики. Саме ці країни безпосередньо відчули близькість загроз (наприклад, популяризація в соціальних мережах Латвії ідеї «Латгальської народної республіки», на кшталт терористичних організації ДНР та ЛНР, звинувачення МЗС РФ у дискримінації Латвією російськомовного населення спонукало прибалтів провести чіткі паралелі з українським питанням) [11].

В умовах спроб переділу сфер впливу Балтія залишається однією з найбільш вразливих ланок європейської безпеки. У разі загострення конфліктних ситуацій на східних кордонах України, а також посилення дипломатичного протистояння щодо Росії, остання демонстративно

намагатиметься нарощувати військову присутність на кордонах з балтійськими країнами.

Найвразливішою з країн Балтії є Естонія, найбільш східне місто якої — Нарва — налічує 90% етнічних росіян. У разі російської агресії в цьому напрямку під сумнів будуть поставлені не лише політичні запевнення щодо безпеки, як це сталося з Будапештським меморандумом, а союзницькі зобов'язання країн-членів НАТО.

За таких умов Україна є важливим стратегічним партнером, який може стати вирішальним у врегулюванні проблеми безпеки в країнах Балтії. Першим практичним кроком у цьому напрямку є налагодження співпраці між Україною, Польщею та Литвою, вигідної для всіх країн регіону Східної Європи.

Досить цікавим у досліджуваному контексті є досвід Ізраїлю. Зокрема розширення у 2018 році повноважень Національного кібердиректорату (National Cyber Directorate, NCD) — провідного державного агентства з питань кібербезпеки [12]. Розширення повноважень стосувалися першочергово оцінки ризиків для національних мереж, планування захисту та відновлення, а також управління державними та приватними структурами. Ці зміни на експертному рівні були оцінені неоднозначно [13]. Проте, як зазначають в Уряді, пояснюється постійним зростанням загроз у кіберсфері.

Цікаво, що в Ізраїлі розділені функції цивільних та військових органів. Так, NCD повинен оцінювати загрози, виявляти уразливі місця в національних системах та обмінюватися інформацією в режимі реального часу, однак у нього немає повноважень вживати заходів у відповідь на атаки. Передбачається, що активні дії у кіберпросторі провадитимуть військові, а також спецслужби Ізраїлю.

У структурі NCD створено два органи: Центр протидії кіберзагрозам (цю функцію виконуватиме команда реагування на комп'ютерні

надзвичайні події CERT-IL) і Центр раннього виявлення та верифікації для попередження про атаки та зменшення їхнього шкідливого впливу. Останній має сприяти обміну даними про ситуацію в інформпросторі між державними та приватними організаціями. Це робитиметься, зокрема, і через створення та наповнення національної бази даних із маркерами загроз. Запропонована база викликала значні суперечки в ізраїльському суспільстві, адже йдеться про збір та обробку великих масивів приватної та корпоративної інформації [12].

Основними правовими документами політики Ізраїлю у сфері кібербезпеки є Національна кіберініціатива 2010 та Резолюція уряду №3611 від 7 серпня 2011 року, яка є планом дій Національної кібер-ініціативи [14].

Слід зауважити, що в Ізраїлі не тільки успішно розвивається сфера кібербезпеки, а й проводяться власні розробки кіберзброї. Такі ініціативи мають за мету створити в Ізраїлі аналог Інтерполу в кіберпросторі, а також запровадити систему обміну інформацією між усіма суб'єктами кіберзахисту у поєднанні зі спроможностями державного та приватного секторів [15, с. 49]. Досвід співпраці державного та приватного секторів у сфері забезпечення кібербезпеки може бути корисним для національної практики.

Таким чином, можна констатувати, що Ізраїль має значні можливості протистояти дедалі більшим кіберзагрозам. Разом з тим, нові положення породжують дискусії, що підкреслює складнощі у підтриманні рівноваги необхідності гарантування національної безпеки та захисту фундаментальних громадянських прав.

Висновки та перспективи подальших досліджень у даному напрямку. Виходячи із аналізу забезпечення кібербезпеки у зарубіжних країнах, зокрема Ізраїлю, вважаємо за доцільне запропонувати окремі напрями вдосконалення національної практики у досліджуваній сфері. Зокрема, доповнити Положення про Національний координаційний центр

кібербезпеки, затверджене Указом Президента України від 7 червня 2016 року № 242/2016 [16] у частині вдосконалення основних завдань даного органу. У цьому контексті пропонується розширити п. 3 вказаного Положення, додавши до основних завдань Центру наступні:

- впровадження в Україні стандартів безпеки мережевих та інформаційних систем;
- визначення критерії в, за якими буде складатись перелік операторів базових послуг та провайдерів цифрових послуг;
- контроль за дотримання мережевої нейтральності та міжнародних та європейських стандартів та заборон введення окремих національних стандартів у сфері кібербезпеки, які не є сумісними з європейськими та міжнародними стандартами;
- аудит системи мережевої та інформаційної безпеки;
- організація та підтримка системи сповіщення про кіберінциденти, системи аудиту та впровадження заходів мережевої та інформаційної безпеки;
- забезпечення належного дотримання вимог щодо збереження конфіденційності, зокрема щодо персональних даних та захисту комерційних інтересів операторів та провайдерів.

В України є свій досвід, коли 2015 року були намагання втрутитися до системи енергопостачання, яка, крім того, включає і ядерну енергетику. Європейські країни, перш за все Німеччина, вже були об'єктами схожих атак. Не менше значення має проведення різних операцій в кіберсфері, спрямованих на перешкоджання нашим демократичним процесам. Ми вже ставали свідками дезінформаційних кампаній проти референдумів, як, наприклад, стосовно Brexit у Великобританії чи Угоди про асоціацію з Україною в Нідерландах. Операції, які покликані підмінити результати волевиявлення, зараз перетворюються на нову норму.

Основна проблема ефективного забезпечення кібербезпеки полягає у створенні в ЄС єдиного європейського політичного простору. Значна активність в цій сфері керівних органів ЄС стикається з нездатністю ряду країн в повному обсязі виконати всі директиви, розпорядження, регламенти та інші нормативні акти. Слід також враховувати, що паралельно з реакцією ЄС на актуальні кіберзагрози безперервно з'являються все нові загрози кібербезпеки, на які держави і наднаціональні структури ЄС не завжди встигають вчасно реагувати. Переважно це відбувається через складні процедури узгодження на національному і наднаціональному рівнях, що вимагає значного часу, а також через несформованість в ЄС єдиного політичного простору. Проте, не дивлячись на ці проблеми, система забезпечення кібербезпеки в країнах ЄС досить швидко розвивається і вдосконалюється, чому сприяє настільки ж швидке накопичення досвіду регулювання і координації дій країн - членів ЄС у сфері кібербезпеки.

При цьому вважаємо за необхідне підкреслити надважливість проблем забезпечення кібернетичної безпеки усіма суб'єктами її забезпечення, як національного так і міжнародного рівня і визначити її як свій пріоритет стратегічного значення. Необхідним є створення команд фахівців-консультантів з питань кібербезпеки на всіх: від захисту комерційних секретів до розробки правової бази та формування державної політики. Питання кібернетичної безпеки має бути окресленим чіткіше, стати більш зрозумілим і вимірюваним. Компанії, які включає критична інфраструктура, повинні нести відповідальність за рівень своєї готовності і захисту., адже припинення діяльності тієї чи іншої організації в сучасних динамічних реаліях може призвести до руйнівних наслідків та загроз національній безпеці держави.

Нам слід покращити наші партнерські відносини у плані обміну набутими знаннями. Україна володіє надзвичайним досвідом практичної реалізації протидії кіберзагрозам. Вона стала кібернетичним фронтом, на

якому Росія проводить випробування своєї нової кіберзброї, яку зможе використовувати її по всьому світу. У зв'язку з цим, підтримка України повинна стати пріоритетним завданням для країн ЄС, оскільки так вони подбають і про власну безпеку. Безумовно, Україна сьогодні має позиціонуватися як потужний форпост європейської безпеки. На нашу думку, визріла потреба переглянути концепції європейської безпеки. Росія своєю загарбницькою поведінкою продемонструвала, що цивілізованими способами неможливо протистояти її агресії. Результати такої діяльності нікчемні. Відповідно, потребують змін основні акценти концепції європейської безпеки. І це стосується, зокрема, світових безпекових процесів.

Література

1. Камчатний М. В. Історія міжнародно-правового регулювання питань, пов'язаних із застосуванням комп'ютерних технологій. URL: http://oaji.net/pdf.html?n=2016/3229-1477308664.pdf
2. EU International Cyberspace Policy. URL: http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm
3. Глобальный индекс кибербезопасности и профили по киберблагополучию: отчет. Женева, ABI Research, 2015. 516 с.
4. Software Management: Security Imperative, Business Opportunity. BSA URL: https://gss.bsa.org/
5. InHope URL: https://www.inhope.org/EN
6. Haeni R. 2016. Cybersecurity: New EU Directive. Published 20.07.2016. URL: https://news.pwc.ch/28616/cybersecurity-new-eu-directive-published/
7. Пантин В. И., Кардава Н. В. Кибербезопасность: проблемы формирования единой политики в Европейском Союзе // Вестник Пермского университета. Политология. 2018. №3. С. 5-17.

8. CYBER RAPID RESPONSE TEAMS AND MUTUAL ASSISTANCE IN CYBER SECURITY. URL: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/
9. Six EU countries unite against cyber threats: the joint Cyber Rapid Response Teams are ready to counter cyber-attacks. Ministry of national defence republic of Lithuania 2020.03.04. URL: http://kam.lt/en/news_1098/current_issues/six_eu_countries_unite_against_cyber_threats_the_joint_cyber_rapid_response_teams_are_ready_to_counter_cyber-attacks.html
10. Šešios ES šalys susivienijo prieš kibernetines grėsmes: atakas atremti pasirengusios jungtinės Greitojo kibernetinio reagavimo komandos. LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJA. URL:http://kam.lt/lt/naujienos_874/aktualijos_875/sesios_es_salys_susivienijo_pries_kibernetines_gresmes_atakas_atremti_pasirengusios_jungtines_greitojo_kibernetinio_reagavimo_komandos.html
11. Ответ официального представителя МИД России А. К. Лукашевича на вопрос СМИ в связи с обращением Центра государственного языка Латвии к жителям страны разговаривать на рабочих местах только на латышском языке / МИД России. URL: http://archive.mid.ru//brp_4.nsf/newsline/F1D4CD9DD330630643257DD7003FD0D7
12. Israel National Cyber Directorate URL: https://www.gov.il/en/departments/israel_national_cyber_directorate
13. A Look at Israel's New Draft Cybersecurity. Blog Post *by* Guest Blogger for Net Politics. Law. July 2, 2018. URL: https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law
14. Cyberwellness Profile Israel URL: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf

15. Гребенюк М.В., Леонов Б.Д. Досвід Ізраїлю у сфері забезпечення кібербезпеки. “Інформація і право. № 2(25)/2018. С. 45-50
16. Положення про Національний координаційний центр кібербезпеки. Указ Президента України від 7 червня 2016 року № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016

References

1. Kamchatnyj M. V. Istorija mizhnarodno-pravovogho reghuljuvannja pytanj, pov'jazanykh iz zastosuvannjam komp'juternykh tekhnologhij. URL: http://oaji.net/pdf.html?n=2016/3229-1477308664.pdf
2. EU International Cyberspace Policy. URL: http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm
3. Ghlobaljnыj yndeks kyberbezopasnosty y profyly po kyberblaghopoluchyju: otchet. Zheneva, ABI Research, 2015. 516 s.
4. Software Management: Security Imperative, Business Opportunity. BSA URL: https://gss.bsa.org/
5. InHope URL: https://www.inhope.org/EN
6. Haeni R. 2016. Cybersecurity: New EU Directive. Published 20.07.2016. URL: https://news.pwc.ch/28616/cybersecurity-new-eu-directive-published/
7. Pantyn V. Y., Kardava N. V. Kyberbezopasnostj: problemы formyrovanyja edynoj polytyky v Evropejskom Sojuze // Vestnyk Permskogho unyversyteta. Polytologhyja. 2018. #3. S. 5-17.
8. CYBER RAPID RESPONSE TEAMS AND MUTUAL ASSISTANCE IN CYBER SECURITY. URL: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/
9. Six EU countries unite against cyber threats: the joint Cyber Rapid Response Teams are ready to counter cyber-attacks. Ministry of national defence republic of Lithuania 2020.03.04. URL:

http://kam.lt/en/news_1098/current_issues/six_eu_countries_unite_against_cyber_threats_the_joint_cyber_rapid_response_teams_are_ready_to_counter_cyber-attacks.html

10. Šešios ES šalys susivienijo prieš kibernetines grėsmes: atakas atremti pasirengusios jungtinės Greitojo kibernetinio reagavimo komandos. LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJa. URL:http://kam.lt/lt/naujienos_874/aktualijos_875/sesios_es_salys_susivienijo_pries_kibernetines_gresmes_atakas_atremti_pasirengusios_jungtines_greitojo_kibernetinio_reagavimo_komandos.html
11. Otvet ofycyaljnogho predstavytelja MYD Rossyy A. K. Lukashevycha na vopros SMY v svjazy s obrashhenyem Centra ghosudarstvennogho jazыka Latvyy k zhyteljam stranы razghovaryvatj na rabochykh mestakh toljko na latыshskom jazыke / MYD Rossyy. URL: http://archive.mid.ru//brp_4.nsf/newsline/F1D4CD9DD330630643257DD7003FD0D7
12. Israel National Cyber Directorate URL: https://www.gov.il/en/departments/israel_national_cyber_directorate
13. A Look at Israel's New Draft Cybersecurity. Blog Post by Guest Blogger for Net Politics. Law. July 2, 2018 URL: https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law
14. Cyberwellness Profile Israel URL: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf
15. Ghrebenjuk M.V., Leonov B.D. dosvid Izrajilju u sferi zabezpechennja kiberbezpeky. “Informacija i pravo. # 2(25)/2018. S. 45-50
16. Polozhennja pro Nacionaljnyj koordynacijnyj centr kiberbezpeky. Ukaz Prezydenta Ukrajiny vid 7 chervnja 2016 roku # 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016