Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Наказ Міністерства освіти і науки України від 22.12.2016 № 1604)
www.dy.nayka.com.ua | № 2 2019 р. | 28.02.2019

DOI: 10.32702/2307-2156-2019.2.5

УДК 351

В. В. Шпачук,
доктор наук з державного управління,
Таврійський національний університет імені В.І. Вернадського

СУБ'ЄКТИ ДЕРЖАВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ КРАЇНИ: ЗАРУБІЖНИЙ ДОСВІД

V. V. Shpachuk
Doctor of Science in Public Administration,
Taurida National University named after V.I. Vernadsky

PUBLIC ADMINISTRATION MANAGERS CYBER SECURITY OF THE COUNTRY: FOREIGN EXPERIENCE

Основою національних систем кібернетичної безпеки більшості країн світу є державні органи, які, відповідно до покладених завдань, безпосередньо виконують функції із забезпечення безпеки кіберпростору. Світовий досвід показує, що близько 70 країн світу на сьогодні активно займаються питаннями кібербезпеки держави, в тому числі у військовій сфері. Близько 50 країн мають власні системи кібербезпеки, які створені за останнє десятиріччя.
Україні також необхідно створити власну ефективну систему державного управління інформаційною безпекою в умовах існуючих та потенційних кіберзагроз з визначенням ключових структур та механізмів у вигляді спеціалізованих установ, центрів, інститутів, спрямованих на ведення інформаційної війни, запобігання та уникнення всіляких кіберзагроз. При цьому, система державного управління кібербезпекою повинна представляти з себе певний формат співробітництва державних органів, установ, організацій, приватного сектору економіки, наукових установ і організацій, професійних асоціацій та неурядових організацій у сфері кібербезпеки, а не певну кількість, хоча і вискокомпетентних та високопрофесійних, відокремлених одна від одної державних установ та організацій. Суб'єкти системи забезпечення інформаційної безпеки України мають тісно взаємодіяти між собою, водночас кожний з них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції, вживаючи при цьому відповідні, визначені законом, адміністративно-правові форми та методи. У результаті такої взаємодії зазначені суб'єкти доповнюють один одного, внаслідок чого утворюють стрункy організаційно-функціональну систему, об'єднану як системою владно-розпорядчих повноважень, так і функцією по забезпеченню інформаційної безпеки.
З огляду на це, у статті представлено результати дослідження найбільш успішного зарубіжного досвіду щодо здійснення організаційних заходів, спрямованих на розбудову ефективних систем державного управління кібернетичною безпекою країн.

The basis of the national systems of cybernetic security in most countries of the world are state bodies, which, in accordance with the assigned tasks, directly perform the functions of security of

cyberspace. World experience shows that about 70 countries of the world are currently actively engaged in cybersecurity of the state, including in the military sphere. About 50 countries have their own cyber security systems that have been established over the past decade.
Ukraine also needs to create its own effective system of state management of information security in the context of existing and potential cyber threats with the definition of key structures and mechanisms in the form of specialized institutions, centers, institutions aimed at conducting information warfare, prevention and avoidance of all kinds of cyber threats. At the same time, the system of public administration of cybersecurity should represent a certain format of cooperation between state bodies, institutions, organizations, the private sector of the economy, scientific institutions and organizations, professional associations and non-governmental organizations in the field of cybersecurity, and not a certain number, although highly qualified and highly professional, separated from each other state institutions and organizations. The entities of the information security system of Ukraine should interact closely with each other, while each of them specializes in solving specific tasks in accordance with its subject-matter competence, while using the corresponding legal and administrative forms and methods defined by the law. As a result of such interaction, these subjects complement each other, resulting in a harmonious organizational and functional system, united as a system of power and regulatory powers, and a function to provide information security.
In view of this, the article presents the results of the study of the most successful foreign experience in implementing organizational measures aimed at developing effective systems of public administration of cybernetic security of countries.

***Ключові слова**: державне управління; кібербезпека; загроза; суб'єкт; установа; система.*

***Key words**: government; cybersecurity; threat; subject; institution; system.*

Постановка проблеми. На сьогодні проблема захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, від викликів і загроз у кібернетичному просторі є однією з найголовніших для будь-якої держави, а забезпечення належного рівня кібернетичної безпеки держави є необхідною умовою забезпечення національної безпеки держави, розвитку інформаційного суспільства. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем державного управління та захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру. У багатьох провідних країнах світу вже сформовані загальнодержавні системи державного управління кібернетичною безпекою – як найбільш оптимальні організаційні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам.

В Україні також відбувається процес формування системи кібернетичної безпеки, тому дослідження і використання передового світового досвіду з цього питання є необхідною умовою для побудови ефективної системи державного управління кібернетичною безпекою України в найкоротші строки.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження різних аспектів інформаційної безпеки та її забезпечення внесли такі вітчизняні та зарубіжні науковці як О. Баранов, В. Богданович, В. Бурячок, М. Грайворонський, І. Діордіца, Д. Дубов, Є. Живило, В. Ліпкан, Н. Логінова, А. Мовчан, О. Черноног, В. Шеломенцев та інші. Вагомий внесок у дослідження кібербезпеки зробили такі зарубіжні вчені, як П. Домровський, А. Клімбург, Дж. Наямол, Г. Раттрей, С. Старр, Д. Шелдон та інші. Нормативно-правові аспекти системи кібернетичної безпеки розглядалися в працях К. Александера, Дж. Ліпмана, В. Мазурова, Р. Олдрича, Є. Старостиної, М. Шмітта, А. Щетилова, серед вітчизняних науковців необхідно відмітити праці В. Бурячка, Р. Грищука, Ю. Даника, О. Довганя, В. Петрова, Т. Тропініної та ін та інших.

Мета дослідження. Метою статті є дослідження зарубіжного досвіду щодо здійснення організаційних заходів, спрямованих на розбудову ефективних систем державного управління кібернетичною безпекою країн.

Виклад основного матеріалу. В умовах глобалізації світової економіки та інформаційного обміну, глобального поширення та впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства проблема захисту інформації постали перед усіма державами світу. Можливості кібернетичного простору створили фундаментальну залежність від нормального функціонування інформаційних технологій всіх сфер життєдіяльності окремих громадян, суспільства та держави: економіки, політики, сфери національної та

міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам і телекомунікаційним системам.

Ключова роль у здійсненні державного управління кібербезпекою Сполучених Штатів Америки належить Міністерству внутрішньої безпеки (МВБ) [1], яке було створене в результаті повного реформування спеціальних служб і силових відомств США після подій 11 вересня 2001 року. Відповідно до прийнятого 25 листопада 2002 року закону США «Про внутрішню безпеку» (Homeland Security Act of 2002) – урядові структури, які займались забезпеченням комп'ютерної безпеки, перейшли під контроль цього Міністерства.

На Міністерство внутрішньої безпеки США покладено завдання із забезпечення державної безпеки США: боротьба з тероризмом, зовнішніми загрозами, забезпечення кібербезпеки, попередження наслідків стихійних лих тощо. Зважаючи на покладені на Міністерство завдання, воно має надзвичайно широкі повноваження та значний бюджет, а до його складу було введено понад 20-ти федеральних агентств і відомств [2]. Саме ж забезпечення кібернетичної безпеки покладено на Управління кібербезпеки та комунікацій Міністерства (Office of Cyber Security and Communications), у складі якого створено Національний центр кібербезпеки та комунікацій (National Cybersecurity and Communications Integration Center [3]. Безпосередніми завданнями Центру є:

- раннє попередження про кібератаку,
- захист від несанкціонованого доступу до комп'ютерних мереж,
- розслідування кіберзлочинів із використанням штату спеціальних агентів,
- координація діяльності федеральних органів влади з реагування на різноманітні комп'ютерні надзвичайні події,
- вжиття оперативних заходів щодо виявлення та локалізації джерела кіберзагроз [4].

Ще одним структурним елементом вказаного підрозділу є Центр екстреного реагування на комп'ютерні інциденти в США (US-CERT), який було утворено у 2004 році і який здійснює заходи зі зміцнення системи національної кібербезпеки, координує обмін інформацією й оперативно протидіє кібернетичним ризикам, що загрожують державі, захищаючи конституційні права американців [5].

В Ізраїлі внаслідок збільшення проявів кібератак з боку ісламських екстремістів У червні 2010 року при службібезпеки (ШАБАК) був створений відділ з інформаційної безпеки, який контролює критично важливі національні інфраструктури, котрі спеціалізуються на запобіганні кібертероризму, проведенні спеціальних операцій в глобальному інформаційному просторі [6]. З метою адекватного реагування на виклики та загрози в кіберпросторі в Ізраїлі прийнято два стратегічних документи: Національна кіберініціатива 2010 року та Резолюція уряду № 3611 від 7 серпня 2011 року, яка запроваджує План дій з реалізації Національної кіберініціативи. На виконання цих нормативно-правових актів у 2012 році урядом був створений Національний кіберштаб для реалізації засад національної кібербезпекової політики і нарощування технологічного потенціалу в кіберпросторі. Також у 2012 році в Ізраїлі була створена кіберполіція як суб'єкт забезпечення національної безпеки [7].

У 2015 році в Ізраїлі було створено Національне управління кібербезпеки (The National Cyber Bureau) як координаційний орган, діяльність якого спрямована на посилення цифрового захисту. Створення цієї структури було зумовлене тим, що в країні спостерігався досить високий рівень комп'ютеризації, що, однак, автоматично провокувало загрозливі тенденції в кіберпросторі, у зв'язку з чим багато державних інституцій та представників комерційного середовища стали уразливими до кібератак. Рішення про доцільність створення двох окремих підрозділів у рамках однієї системи пояснюється необхідністю здійснювати діяльність у двох напрямах: стратегічному, у рамках якого формується державна політика і нарощуються технологічні потужності, і оперативному, який використовує напрацювання Штабу. Крім цього, відповідно до резолюції № 2444 від 15 лютого 2015 року та рекомендацій Національного кіберштабу, уряд Ізраїлю схвалив рішення про створення ще й Національного управління з кіберзахисту як центрального оперативного органу Національного кіберштабу.

З метою інституційної оптимізації процесів забезпечення кібербезпеки 17 грудня 2017 року ізраїльським урядом було прийнято рішення про об'єднання Національного кіберштабу і Національного управління з кіберзахисту в єдину Національну службу кібербезпеки, яка на сьогодні відповідає за всі аспекти кіберзахисту: від формування засад державної політики та нарощування технологічних потужностей до оперативної роботи спеціальних підрозділів, а також за усі аспекти кібероборони в цивільному секторі з метою налагодження ефективної координації та взаємодії між державою та приватним сектором [8].

Головним державним органом Великобританії, на який покладено завдання захисту критичної інфраструктури, мінімізації загроз сталому її функціонуванню, насамперед від загроз тероризму, є Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI). Центр – це міжвідомча організація, яка підпорядкована та фінансується Службою безпеки Великобританії (MI-5), контррозвідувальним органом країни, що здійснює заходи забезпечення захисту держави від загроз національній безпеці (тероризму, шпигунства, поширення зброї масового знищення). Директор CPNI підзвітний генеральному директору MI-5 та діє відповідно до закону «Про Службу безпеки» 1989 року [9].

Крім того, у Великобританії у зв'язку із збільшенням кількості кібернетичних атак на комп'ютерні мережі країни та за ініціативи урядових структур спільно з великими приватними компаніями наприкінці березня 2013 року на базі існуючої системи партнерства та обміну інформацією з питань кібернетичної безпеки (Cyber Security Information Sharing Partnership, CISP), яка діє в країні з 2012 року, було створено Центр з протидії кібернетичним загрозам. Метою створення Центру є:

по-перше, попередження та нейтралізація кібернетичних атак на об'єкти критичної інфраструктури,

по-друге, швидке реагування на скоєні правопорушення у цій сфері.

Досліджуючи зарубіжний досвід забезпечення кібербезпеки, не можна не звернути увагу на країну–сусіда Польщу, яка на сьогодні активно займається розвитком кіберзахисту на державному рівні [10]. Тривалий час зусилля влади Польщі щодо боротьби з кіберзагрозами були недостатніми. У 2011 році у Польщі було створене Міністерство адміністрації і цифровізації, завданнями якого стали забезпечення кібербезпеки у військовій сфері, захист конфіденційності громадян, побудова національної освітньої платформи, залучення до Інтернету людей похилого віку і жителів віддалених районів країни. В рамках Міністерства цифровізації у 2016 році створили Національний центр кібербезпеки. Його ключовим завданням стало попередження загроз, реакція на них та координація дій.

До завдань Міністерства адміністрації і цифровізації Польщі відносяться:

- розробка та реалізація стратегічних документів і правових актів в області кібербезпеки,
- проведення національного і міжнародного співробітництва,
- розробка керівних принципів для створення відповідних заходів щодо захисту інформаційних систем,
- підготовка аналізу щодо стану кібербезпеки на національному рівні та ризиків для держави кібербезпека,
- розробка центральних навчальних планів, вправ та випробувань [11].

Викликає зацікавленість досвід з формування систем державного управління кібербезпекою країн Прибалтики. Серед основних причин зацікавленості в їх досвіді слід виділити наступні:

по-перше, зазначені країни, як і Україна. Є республіками колишнього СРСР і тому мають в більшості сфер однакові початкові умови;

по-друге, зазначені країни, як і Україна, зазнали кібератак на власні інформаційні системи з боку Російської Федерації, під час ведення останньої гібридної війни проти них (Естонія першою з країн пострадянського простору зазнала кібератак на власні інформаційні системи ще навесні 2007 року під час російсько-естонського політико-дипломатичного скандалу).

Так, ще у 2004 р. Республіка Естонія вступила до Європейського Союзу та стала країною-членом Північноатлантичного Альянсу, що обумовило розвиток цього напряму відповідно до керівних документів ЄС і НАТО і, як результат уже у 2006 році в країні для був заснований Центр реагування на комп'ютерні інциденти. У 2009 році у рамках Комітету з питань безпеки при Уряді Республіки Естонія була створена Рада з кібербезпеки, основне завдання якої полягає в розвитку стратегічного рівня співпраці між різними міністерствами й відомствами країни та контроль за реалізацією Стратегії кібербезпеки країни. Державну політику Естонії у сфері кібербезпеки нині спрямовує та координує Міністерство економіки та комунікацій. Розвиток державних інформаційних систем і розслідування інцидентів у сфері захисту кібербезпеки організовує Департамент державних інформаційних систем цього Міністерства.

У 2010 році за рішенням Уряду, Естонському центру інформатики було надано статус урядового органу та перейменовано в Estonian Information System Authority (Riigi Infosiisteemi Amet - RIA), він отримав додаткові повноваження й можливості для організації захисту державної інформаційно-комунікаційної інфраструктури і здійснення контролю за безпекою інформаційних систем. RIA організаційно підпорядковується Міністерству економіки та комунікацій Республіки Естонія та виконує низку завдань, серед яких: організація діяльності, пов'язаної з державним інформаційними системами та інформаційною безпекою естонської критичної інформаційної інфраструктури; контроль за виконанням вимог законодавства, яке регулює управління інформаційними системами держави; підготовка міжнародних проектів та участь у них [12].

У рамках RIA було сформовано окрему структуру - Департамент із захисту критичної інформаційної інфраструктури (далі - CIIP), безпосереднім завданням якого є організація захисту об'єктів критичної інфраструктури. У 2011 р. із числа менеджерів з кібербезпеки та служб життєзабезпечення було створено комісію CIIP для розвитку державно-приватного співробітництва. Завдання цієї структури - організація обміну оперативною інформацією, виявлення проблем і розробка пропозицій щодо поліпшення кібербезпеки ключової інфраструктури країни. У сфері кібербезпеки основною організацією, відповідальною за проведення навчання й підвищення рівня інформування про кіберінциденти є Фонд розвитку освіти у сфері інформаційних технологій (HITSA), раніше відомий як Фонд "Стрибок тигра" [13].

У 2012 р. відділи Департаменту поліції та прикордонної охорони (PBGB) з розслідування кіберзлочинів були об'єднані в єдиний департамент. Окрім цього, посадові особи, відповідальні за виявлення кіберзлочинів і роботу з електронною доказовою базою, були об'єднані у службу з розслідування кіберзлочинів та обробки електронних доказів, які стали діяти в префектурах з 2013 р. PBGB також були залучені до інформування про кіберзагрози, що в подальшому обумовило заснування посади web-констеблів (поліціянти, які працюють в

інтернеті). Завдання web-констебля полягає в підвищенні обізнаності про безпеку інтернету й захисту дітей та молоді в режимі онлайн [14].

Служба внутрішньої безпеки Республіки Естонія постійно вдосконалює свої можливості щодо запобігання загрозам національній безпеці, зокрема, щодо кібератак та кібершпигунства. Створення кіберпідрозділів в Естонській лізі оборони (далі - EDL CU) – національній організації-волотері, яке сталося в результаті співпраці між державою, приватним сектором і третім сектором, стало інструментом забезпечення національної оборони. Досвід волонтерів EDL CU застосовується для поліпшення безпеки інформаційних систем естонських державних органів і приватних підприємств за допомогою проведення занять і тестування. EDL CU також може залучатися для підтримки громадських інститутів і захисту інфраструктури в кризовій ситуації [15].

Щодо Литовської Республіки, то у грудні 2014 р. сейм Литви прийняв Закон "Про кібернетичну безпеку", яким було передбачено створення Національного центру кібернетичної безпеки, відкриття якого відбулось 12 липня 2016 р. на території Литовської військової академії ім. генерала Йонаса Жемайтиса. У рамках своєї компетенції новостворений Центр разом із державними установами, організаціями та іншими суб'єктами вирішуватиме питання кібернетичної безпеки державних інформаційних ресурсів та інформаційної інфраструктури особливого призначення [16].

З 1 січня 2018 р. у Литві розпочала діяти нова системи національної кібернетичної безпеки, а також служба інформаційної безпеки, в структтурі якої створено три киберпідрозділи (модулі кібернетичної оборони та управління мережами чисельністю 20 фахівців), що підпорядковані Міністерству оборони. Перший модуль - постійної бойової готовності - складається з професійних військовослужбовців, тоді як два інших складаються з резервістів, які за потреби будуть включені в загальну діяльність.

У 2011 р. у Латвії було прийнято Закон "Про безпеку інформаційних технологій", згідно з яким було утворено Раду з безпеки інформаційних технологій, до обов'язків якої відноситься вироблення стратегії розвитку кібербезпеки на державному рівні, координації розвитку політики кібербезпеки. Рада з безпеки інформаційних технологій виконує функцію центрального координуючого органу для обміну інформацією та співробітництва між державним та приватним сектором Латвії [17].

За рішенням Кабінету міністрів Республіки Латвія від 16 квітня 2013 р. Міністерство оборони прийняло керівництво Національною Радою з питань безпеки інформаційних технологій і в її рамках за участю суспільства та представників недержавних організацій продовжило діяльність з розробки основних документів. Затверджено Перелік інформаційних ресурсів особливої важливості. У Міністерстві оборони здійснено консолідацію функцій та служб кібернетичної безпеки та електронного захисту держави [16].

Так, Міністерство оборони координує розвиток та впровадження інформаційних технологій, політику безпеки та захисту, а також співпрацює в забезпеченні міжнародного співробітництва; Секція координації політики кібернетики МО організовує та надає підтримку щодо впровадження політики кібербезпеки. Міністерство закордонних справ координує міжнародне співробітництво, співпрацю та участь Латвії в різних міжнародних ініціативах, пов'язаних із кібербезпекою.

Комісія з фінансового та капітального ринків регулює і контролює діяльність у кіберпросторі членів міжнародного ринку кіберпростору; Банк Латвії сприяє безпеці та роботі платіжних систем. Міністерство економіки відповідає за економічний розвиток політики кібербезпеки. Міністерство внутрішніх справ, Державна поліція та Поліція безпеки реалізують політику боротьби зі злочинністю. Експлуатацію Центру безпечного інтернету Латвії (NetSafe) забезпечує Латвійська інтернет-асоціація, яка покликана навчати суспільство онлайн можливих ризиків та загроз і сприяти використанню безпечного інтернет-контенту. Національні збройні сили та Блок кіберзахисту надають підтримку у кризових ситуаціях [18].

30 липня 2014 р. наказом міністра оборони внесено зміни до організаційної структури Національних збройних сил та створено підрозділ з кібербезпеки - Emerson Security шляхом залучення представників приватного сектора та державних структур. Основною метою підрозділу є розвиток потенціалу для надання підтримки щодо запобігання кіберінцидентам та надання допомоги в разі недостатніх можливостей CERT.LV для мінімізації наслідків кіберінцидентів. У цьому ж році було затверджено Концепцію кіберпідрозділу [19].

Основним завданням Інституту реагування на інциденти в галузі інформаційних технологій (CERT.LV) є організація інформаційних та освітніх заходів для державних службовців, фахівців з інформаційної безпеки громадськості. CERT.LV відповідає за безпеку в усьому електронному інформаційному просторі. CERT.LV діє в підпорядкуванні Міністерству оборони Латвійської Республіки, його діяльність регулюється Законом Латвійської Республіки "Про захист інформаційних технологій" [20].

Висновки. На сьогодні світові тенденції розвитку інформаційного суспільства спонукають всі держави світу для прийняття заходів щодо забезпечення кібербезпеки. Не є виключенням і Україна, яка нині знаходиться лише на перших етапах розвитку цього інституту.

Здійснене дослідження зарубіжного досвіду щодо здійснення організаційних заходів, спрямованих на розбудову ефективних систем державного управління кібернетичною безпекою країн дозволило зробити висновок що система кіберпезпеки країни передбачає наявність окремого центрального державного органу, який формує інформаційну політику, здійснює законотворчу та нормативну діяльність у цій сфері, координує діяльність інших міністерств, відомств, забезпечує взаємодію із приватним сектором, опікується

питаннями міжнародного співробітництва щодо протидії кіберзлочинності, організує систему інформування та оповіщення населення з проблем кібербезпеки.

У процесі формування системи захисту національної інфраструктури від кіберзагроз неабияке значення має організація взаємодії державного і приватного секторів. Найбільш ефективною така взаємодія є у країнах, де вона будується на довірчих, а не імперативних засадах – приватний сектор заохочується до співпраці шляхом надання певних привілеїв.

Список використаних джерел.

1. Siobhan G. NSA Chief Seeks Bigger Cybersecurity Role // The Wall Street Journal, vol. 8, [Електронний ресурс]. – Режим доступу : http://www.wsj.com/articles/SB10001424052970203833004577247710881763168 (дата звернення: 22.12.2018).
2. Иванов В. США продолжают созидать киберстену // Независимое военное обозрение, № 15, [Електронний ресурс]. – Режим доступу : http://nvo.ng.ru/spforces/2010-04-09/15_cyberwall.html (дата звернення: 12.01.2019).
3. Структура органов государственной власти, обеспечивающих информационную безопасность в США [Електронний ресурс]. – Режим доступу : http://www.intuit.ru/studies/courses/563/419/lecture/9576?page=2 (дата звернення: 22.12.2018).
4. About National Cybersecurity and Communications Integration Center [Електронний ресурс] // Офіційний сайт Міністерства внутрішньої безпеки США. – Режим доступу : https://www.dhs.gov/about-national-cybersecurity-communications-integration-center (дата звернення: 24.12.2018).
5. About Us [Електронний ресурс] // Офіційний сайт Міністерства внутрішньої безпеки США. – Режим доступу : United States Computer Emergency Readiness Team, official web site, http://www.uscert.gov/about-us (дата звернення: 24.12.2018).
6. Спецслужбы Израиля – список специальных подразделений. – Режим доступу : http://www.pro-israel.ru/specslujbi-israelya.html (дата звернення: 25.12.2018).
7. В Израиле появилась Национальная система кибербезопасности – Режим доступу : http://mignews.com/news/politic/171217_221926_94739.htm. (дата звернення: 25.12.2018).
8. Израиль вошел в ТОП-10 стран по уровню кибервойск. – Режим доступу : https://stmegi.com/posts/41238/izrail-voshel-v-top-10-stran-po-urovnyu-kibervoysk (дата звернення: 25.12.2018).
9. Бик В.В. Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз : моногр. / В.В. Бик, А.А. Климчук, В. Н. Панченко, В. В. Петров. – К. : Академпресс, 2013. – 55 с.
10. Кібербезпека: віртуальна зброя держави. URL: https://biz.nv.ua/ukr/experts/kutsenko1/kiberbezpeka-zbroja-derzhavi-u-virtualnij-ploshchini-2014774.html. (дата доступу – 10.01.2019).
11. Cyberbezpieczeństwo / Ministerstwo Cyfryzacji Official website. URL: https://www.gov.pl/cyfryzacja/cyberbezpieczenstwo (дата звернення: 28.12.2018).
12. Information System Authority [Електронний ресурс]. - Режим доступу : https://www.ria.ee/en/about-estonian-information-system-authority.html. (дата звернення: 28.12.2018).
13. Information Technology Foundation for Education [Електронний ресурс]. - Режим доступу: http://www.hitsa.ee/about-us (дата звернення: 28.12.2018).
14. Critical Information Infrastructure Protection [Електронний ресурс]. - Режим доступу : https://www.ria.ee/en/ciip.html (дата звернення: 06.01.2019).
15. History of the EDL CU [Електронний ресурс]. - Режим доступу : http://www.kaitseliit.ee/en/history-of-the-edl-cu (дата звернення: 06.01.2019).
16. Кибернетическая безопасность: ситуация в Литве и странах Балтии [Електронний ресурс]. - Режим доступу : https://net-artis.com/kiberneticheskaya-bezopasnost-situaciya-v-litve-i-stranax-baltii/ (дата звернення: 06.01.2019).
17. Cyber security strategy of Latvia 2014-2018 [Електронний ресурс]. - Режим доступу : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (дата звернення: 06.01.2019).
18. Гапеєва О. Л. Інформаційне протистояння між Росією та Естонією на прикладі подій "Бронзової ночі" 2007 р. / О. Л. Гапеєва // Військово-історичний меридіан. - 2017. - № 15. - С. 86-98.
19. Zemessardzes Kiberaizsardzī bas vienī ba [Електронний ресуср]. - Режим доступу : http://www.zs.mil.lv/Zemessardzes%20vienibas/kiberaizsardzibas_vieniba.aspx (дата звернення: 07.01.2019).
20. Nacionāl o bruņ oto spē ku kiberaizsadzī bas vienī bas (kav) koncepcija [Електронний ресурс]. - Режим доступу : http:// www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/%20cyberzs_April_2013.ashx (дата звернення: 08.01.2019).

Referenses.

1. Siobhan, G. (2012), "NSA Chief Seeks Bigger Cybersecurity Role", *The Wall Street Journal,* [Online], vol. 8, available at: http://www.wsj.com/articles/SB10001424052970203833004577247710881763168 (Accessed 22 December 2018).

2. Ivanov, V. (2010), "USA continues to build cyberspace”, *Nezavisimoye voyennoye obozreniye,* [Online], vol. 15, available at: http://nvo.ng.ru/spforces/2010-04-09/15_cyberwall.html (Accessed 12 January 2019).

3. INTUIT (2018), "Structure of government bodies providing information security in the US“, available at: http://www.intuit.ru/studies/courses/563/419/lecture/9576? page=2 (Accessed 22 December 2018).

4. The official website of the US Department of Homeland Security (2017), “About the National Cybersecurity and Communications Integration Center“, available at: https://www.dhs.gov/about-national-cybersecurity-communications-integration-center (Accessed 24 December 2018).

5. The official website of the US Department of Homeland Security (2016), “About Us“, available at: http://www.uscert.gov/about-us (Accessed 24 December 2018).

6. pro-israel.ru (2018), “Israeli special services are a list of special units“, available at: http://www.pro-israel.ru/specslujbi-israelya.html (Accessed 25 December 2018).

7. Mignews (2018), “The National Cybersecurity System“, available at: http://mignews.com/news/politic/171217_221926_94739.htm (Accessed 25 December 2018).

8. STMEGI (2017), “Israel has entered the TOP-10 countries in terms of cyber warfare“, available at: https://stmegi.com/posts/41238/izrail-voshel-v-top-10-stran-po-urovnyu-kibervoysk (Accessed 25 December 2018).

9. Byk, V. (2013), *Formirovaniye organizatsionno-pravovoy sistemy zashchity natsional'noy infrastruktury ot kiberugroz* [Formation of the organizational-legal system for the protection of national infrastructure against cyber threats], Akadempress, Kyiv, Ukraine.

10. Kutsenko, S. (2017), “Cyber security: virtual weapon state“, available at: https://biz.nv.ua/ukr/experts/kutsenko1/kiberbezpeka-zbroja-derzhavi-u-virtualnij-ploshchini-2014774.html (Accessed on 10 January 2019).

11. Ministry of Digital Affairs (2016), “Cyber security“, available at: https://www.gov.pl/cyfryzacja/cyberbezpieczenstwo (Accessed 28 December 2018).

12. Information System Authority (2018), available at: https://www.ria.ee/en/about-estonian-information-system-authority.html (Accessed 28 December 2018).

13. Information Technology Foundation for Education (2018), “Information Technology Foundation for Education (2018), available at: http://www.hitsa.ee/about-us (Accessed 28 December 2018).

14. Information System Authority (2018), “Critical Information Infrastructure Protection”, available at: https://www.ria.ee/en/ciip.html (Accessed 06 January 2019).

15. Estonian Defence League (2018), “History of the EDL CU“, available at: http://www.kaitseliit.ee/en/history-of-the-edl-cu (Accessed 06 January 2019).

16. Sapetkajte, V. (2012), “Cybernetic security: the situation in Lithuania and the Baltic States“, available at: https://net-artis.com/kiberneticheskaya-bezopasnost-situaciya-v-litve-i-stranax-baltii/ (Accessed 06 January 2019).

17. European Union Agency for Cybersecurity(2013), “Cyber security strategy of Latvia 2014-2018“, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (Accessed 06 January 2019).

18. Hapeeva, O.L. (2017), “Information confrontation between Russia and Estonia on the example of "Bronze Night", Viyskovo-istorychnyy merydian, vol. 15., pp. 86-98.

19. National Guard (2018), “Cyber Defense Unity“, available at: http://www.zs.mil.lv/Zemessardzes%20vienibas/kiberaizsardzibas_vieniba.aspx (Accessed 07 January 2019).

20. Ministry of Defence develops National Defence Policy(2013), “National Armed Forces Cybercrime Unit (CA) concept“, available at: http: www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncep cijas /% 20cyberzs_April_2013.ashx (Accessed 08 January 2019).

Стаття надійшла до редакції 19.02.2019 р.