УДК 94 [327.019.52(47:474):001:061.1]"2004/2016"
DOI: 10.21847/1728-9343.2017.6(152).120038

ГАПЄЄВА ОЛЬГА,
кандидат історичних наук, старший науковий співробітник, докторант,
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів

ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ У КРАЇНАХ БАЛТІЇ: ІСТОРИЧНА РЕТРОСПЕКТИВА

У статті розглядаються особливості становлення національних систем забезпечення кібернетичної безпеки країн Балтії в історичній ретроспективі з урахуванням положень документів Європейського Союзу та НАТО у цій сфері. Хронологічні рамки дослідження охоплюють період із 2004 до 2016 року.

Показано, що країни Балтії тривалий час перебувають в епіцентрі інформаційних (кібернетичних) атак з боку Російської Федерації. Про це свідчить змістовий аналіз російськомовного контенту в інформаційному просторі прибалтійських країн та звітний матеріал спецслужб Латвії, Литви та Естонії, розміщений на офіційних web-сайтах цих інституцій.

Ключові слова: *інформаційна безпека; інформаційна загроза; кібербезпека; кіберстратегія; національна безпека; країни Балтії.*

Постановка проблеми. Після розпаду СРСР у прибалтійських країнах було створено низку державних інституцій для "відновлення історичної справедливості" та оцінки наслідків діяльності окупаційних режимів. Російська Федерація (далі - РФ) ініціювала роботу міждержавних історичних комісій з метою обговорення проблемних питань спільного історичного минулого країн Балтії та РФ, які виникли впродовж перебування у складі Радянського Союзу. Проте вивчення діяльності цих комісій та аналіз досліджень російських науковців із означеної проблематики переконливо свідчить: ідеться про викривлення історичних фактів, пропагандистське забарвлення наукових студій, звинувачення прибалтійських науковців у політизації історичного минулого та просуванні "окупаційної концепції". Наріжним каменем, який детермінує конфліктність між РФ та країнами Балтії, залишається діаметрально протилежне тлумачення подій 1939-1940 рр. та ставлення до звільнення Латвії, Литви та Естонії від нацистської окупації [1].

Поряд із цим, Російська Федерація тривалий час проводить інформаційну політику, спрямовану на формування негативного іміджу країн Балтії на міжнародній арені. Як свідчить порівняльний аналіз російськомовного контенту в інформаційному просторі прибалтійських країн, до цієї діяльності, окрім працівників сфери масової комунікації, залучені також відомі російські науково-дослідні інституції та окремі представники наукової громадськості [2].

Президент Литви Даля Грибаускайте (Dalia Grybauskaite) висловила припущення, що країни Балтії стикаються з одноманітними безпековими викликами, оскільки перебувають в епіцентрі кібернетичних та інформаційних атак з боку РФ. Підтвердження цих слів ми знаходимо у звітних матеріалах щодо загроз у сфері національної безпеки, розміщених на офіційних сайтах спеціальних служб країн Балтії впродовж останніх трьох років.

Зокрема, у щорічному звіті Поліції безпеки Латвії за 2014 р. відмічається посилення діяльності спецслужб РФ у російськомовному середовищі під гаслом захисту прав співвітчизників. Ця тенденція зберігається й у наступні 2015-2016 роки: у звіті за 2016 р. відзначається високий рівень активності спецслужб РФ, зокрема, зацікавленість питаннями безпеки й оборони країни, суспільними процесами, діяльністю НАТО на території Латвії, відносинами між окремими етнічними групами тощо. Окрім цього, латвійські спецслужби вкотре спостерігають помітну активізацію діяльності в російськомовному молодіжному середовищі. З метою консолідації останніх застосовується пропагандистський термін "российские соотечественники" [3].

У Щорічнику Естонського департаменту інформації "International Security and Estonia" [4] стверджується, що РФ здійснює інформаційні кампанії проти країн-членів НАТО та ЄС шляхом поширення деструктивної інформації за допомогою ЗМІ та соціальних мереж [1, с. 17]. "Росія послідовно поширює тезу, що Естонія, Латвія і Литва не поважають права своїх російськомовних мешканців і фальсифікують історію. Балтійським країнам створюється імідж недемократичних і проблемних партнерів, з метою послаблення їхнього зв'язку із союзниками та скорочення їхньої ролі у формуванні зовнішньої політики щодо Росії. Порушення прав російськомовного населення позиціонується у якості "етнокультурного геноциду" у формі "неонацистських настроїв", - ідеться в доповіді [4, с. 19].

У звіті Департаменту державної безпеки Литви за 2014 р. ідеться про розповсюдження неприйнятної для цієї держави інформації, ведення розвідки з території РФ і Республіки Білорусь (далі - РБ), спрямованої на військову та інші інфраструктури країни, електронної розвідки та кібернетичного шпіонажу. Упродовж 2014 р. основними методами інформаційних впливів з боку РФ були: розповсюдження дезінформації про зовнішню і внутрішню політику Литви, дискредитація членства останньої у ЄС та НАТО, поширення думки про недосконалість Литви як держави, маніпуляція історичними подіями та проблематикою національних меншин. Також активізувалась робота в молодіжному російськомовному середовищі.

В аналогічному звіті за 2015 р. литовські фахівці

відзначають підвищений рівень загрози для країни через збільшення рівня військової співпраці між РФ і РБ, що сприяло активізації спецслужб РБ на території Литви та активної підтримки ними литовських опозиційних сил і рухів.

У 2016 р. РФ знову визнана основною загрозою національній безпеці Литви через військову активність, мілітаризацію Калінінградської області, а також посилення провокацій, у т. ч. проведення кібернетичних й інформаційних атак. Проте російська пропагандистська діяльність не знаходить підтримки серед литовського населення. Так, у Литві на три місяці було зупинено передачу балтійської версії російського Першого каналу через трансляцію передачі із циклу "Людина і закон", у якій була представлена неприйнятна для литовського суспільства версія подій 13 січня 1991 р., що відбулись біля вільнюської телебашти та призвели до загибелі людей.

Підсумовуючи вищевикладене, зазначимо, що основною загрозою національній безпеці країн Балтії є пропагандистська діяльність РФ в інформаційній сфері та її деструктивна діяльність в інформаційному просторі. Слід зауважити, що неодноразові спроби російських науковців переписати історію країн Балтії, фальсифікація та пропаганда нагадують російський сценарій напередодні анексії Кримського півострова та військової агресії на сході України.

На зустрічі лідерів країн у Таллінні, які відбулись 29 вересня 2017 р., президент Литви запропонувала створити європейський "кібернетичний Шенген" та кібернетичні сили швидкого реагування, адже кібератаки загрожують "цифровій" економіці ЄС. У цьому ж контексті висловився й голова Комітету з національної безпеки і оборони сейму Литви Вітаус Бакас - він заявив про необхідність удосконалення кіберзахисту держави, а в подальшому виділити на потребу оборони більш ніж 2 % ВВП.

Кібернетична безпека є складовою інформаційної безпеки держави, оскільки пов'язана із захистом передусім систем управління, ІТ-систем. Інформаційна безпека особи й суспільства є складовою національної безпеки. Навесні 2007 р., під час російсько-естонського політико-дипломатичного скандалу, більш відомого як "Бронзова ніч", Естонія першою з країн пострадянського простору зазнала кібератак на власні інформаційні системи, що спричинило негативні наслідки, зокрема, для банківської сфери. Грузія під час російсько-грузинської війни 2008 р. також зіткнулася з кібератаками з РФ. Наша країна є об'єктом постійних кібератак з боку "східного сусіда", у зв'язку з чим 5 грудня 2017 р. прийнято відповідний Закон України "Про основні засади забезпечення кібербезпеки України". Отже, тематика нашої наукової студії є актуальною й сучасною.

Аналіз останніх досліджень і публікацій. У наших попередніх наукових студіях [1, 2] було розглянуто особливості інформаційного протистояння між РФ та Естонією на прикладі подій квітня 2007 р. та проаналізовано історико-ментальні складові конфліктності між країнами Прибалтики та РФ, досліджено форми й методи деструктивного впливу, що здійснює РФ в інформаційному просторі країн Балтії, зокрема щодо фальсифікації історичних подій, наукові доробки російських учених, здебільшого присвячені становищу російськомовного населення, політиці прибалтійських країн щодо нього та перспективі міждержавних відносин у Прибалтійському регіоні, а також питання історичної пам'яті та історичної політики.

Зауважимо, що в українській історіографії немає цілісного дослідження щодо новітньої історії прибалтійських країн.

Метою статті є виявлення та аналіз особливостей становлення національних систем забезпечення кібернетичної безпеки країн Балтії в історичній ретроспективі.

Виклад основного матеріалу. Перші дослідження з питань кібернетичної безпеки в Естонії припадають на 1991 р. - розробку цієї проблематики здійснювали фахівці Інституту кібернетики Естонії. Але у 2004 р. Республіка Естонія вступила до Європейського Союзу (далі - ЄС) та стала країною-членом Північноатлантичного Альянсу, що обумовило розвиток цього напряму відповідно до керівних документів ЄС і НАТО. У 2006 р. для координації оперативної співпраці був заснований Центр реагування на комп'ютерні інциденти (CERT) і досягнуто домовленості щодо спільної програми державного та приватного секторів - Public-Private Computer Protection 2009.

Як уже йшлося вище, навесні 2007 р., під час російсько-естонського політико-дипломатичного скандалу, Естонія першою з країн пострадянського простору зазнала кібератак на власні інформаційні системи. Саме тому у 2008 р. з метою забезпечення захисту інформаційних систем від кібератак та безпеки країни в інформаційній сфері була розроблена Стратегія кібербезпеки Республіки Естонія (Cyber Security Strategy by Ministry of Economic Affairs and Communication) терміном на п'ять років - до 2013 р. [5]. "Естонія могла б стати в цьому прикладом для інших держав і зайняти світовий форпост не тільки в галузі розвитку електронних послуг, а й у галузі високого рівня безпеки інформаційних систем", - так прокоментував документ Міністр оборони Республіки Естонія Я. Аавіксоо [6].

У розробці Стратегії кібербезпеки брала участь комісія, створена при Міністерстві національної оборони, до складу якої увійшли експерти з усіх міністерств і відомств країни, у тому числі Міністерства економіки і комунікацій, Міністерства внутрішніх справ, Міністерства закордонних справ, Міністерства юстиції, Міністерства освіти і науки, Сил оборони, Державного центру розвитку інформаційних систем та естонського центру CERT, а також представники приватного сектора. При розробці Стратегії було враховано зарубіжний досвід і рекомендації Європейського Союзу та Альянсу [5].

У 2009 р. 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 [Там само].

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 [Там само].

У 2010 р. 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 державними

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 [7].

На початку 2010 р. RIA розпочало відпрацювання картографічної продукції з метою позначення місць розташування об'єктів критичної інформаційної інфраструктури. Результатом роботи стало вироблення вимог для забезпечення безпеки й функціонування інформаційно-комунікаційних систем.

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 [Там само].

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" [8].

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 [9].

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 [10].

Одним із напрямів діяльності кіберпідрозділів є проведення навчань і тренувань з внутрішньої та міжнародної кібербезпеки. Так, у 2012 р. були проведені навчання підрозділів кіберзахисту під керівництвом Уряду Республіки, такі як "Cyber Fever" і навчання країнчленів НАТО з урегулювання кризових ситуацій "CMX-2012" [11].

Наприкінці листопада 2013 р. в Естонії було проведено найбільші навчання з відпрацювання питань кіберзахисту, у яких узяли участь і представники Альянсу - "Cyber Coalition-2013" із залученням більш ніж 500 осіб: співробітників талліннського Об'єднаного центру передового досвіду в галузі кіберзахисту НАТО й офіцерів із більш ніж тридцяти країн-членів і партнерів НАТО у віддаленому доступі [Там само].

Щороку в Естонії проводяться навчання Експертного центру НАТО щодо спільного кіберзахисту (NATO CCD COE) "Locked Shields" (зімкнуті щити). Сили оборони Республіки Естонія також створили майдачник для проведення навчань з кіберзахисту "Cyber Range" ("Кібердіапазон"), який використовується для проведення й організації внутрішніх навчань за планами, розробленими в цивільних вишах.

У 2013 р. розпочалась реалізація проекту державно-приватного партнерства, спрямованого на підвищення навичок та інформованості про безпеку серед користувачів, розробників і продавців смарт-пристроїв.

У 2014 р. затверджено нову редакцію Стратегії кібербезпеки Республіки Естонія на 2014-2017 рр. (Cyber Security Strategy by Ministry of Economic Affairs and Communication). У Стратегії насамперед підсумовано здобутки країни у сфері забезпечення кібербезпеки за попередній період; надано ґрунтовну оцінку викликів і загроз у сфері забезпечення кібербезпеки та зазначено перелік заходів для ефективної боротьби з цими загрозами. Документ продовжує реалізацію цілей, закладених у Стратегії 2008 р. та доповнений новими загрозами й викликами відповідно до реалій сьогодення [12].

В Естонії розташований найбільший на території Європи кіберполігон, на якому щорічно проводять тренінги для фахівців із різних країн. Під час саміту НАТО в Уельсі у 2014 р., у рамках якого було прийнято рішення про створення групи швидкого реагування на випадок агресії з боку Росії, досягнуто й домовленість про виділення фінансування для діяльності естонського кіберполігону і його перехід під управління НАТО. Талліннським університетом технологій (TUT) спільно з Тартуським університетом у 2009 р. розроблена й відкрита міжнародна програма магістратури у сфері кібербезпеки, до якої щорічно приєднуються 50 студентів. У 2014 р. TUT спільно з Естонським центром у сфері кіберзлочинності (2CENTRE) відкрив програму магістратури у сфері цифрової криміналістики [13].

Естонія успішно розвиває співпрацю з іншими країнами й міжнародними організаціями у сфері кібербезпеки. Співпраця у сфері кібербезпеки успішно розвивається також і на регіональному рівні між країнами Північної Європи та балтійськими країнами, а також з іншими стратегічними партнерами. Естонія бере участь у новітніх формах співпраці - онлайн-коаліції "Свобода", Групі урядових експертів ООН, неофіційній робочій групі ОБСЄ з розробки заходів щодо зміцнення довіри до кіберпростору, навчання "Cyber Coalition-2015" проводять учасники з більш ніж 35 країн НАТО і країн-партнерів [10]. Естонський експертний центр 2CENTRE є частиною експертних центрів Європейського Союзу 2CENTRE, професіонали яких проходять навчання з боротьби з кіберзлочинністю [14].

У квітні 2015 р. Пентагон презентував нову Стратегію кібербезпеки (The Department of Defense Cyber Strategy), яка містить три головних напрями діяльності: 1) захист власних інформаційних систем від хакерських атак; 2) співпраця з іншими агентствами й зарубіжними союзниками в напрямку збору інформації розвідувального характеру, спільні операції ФБР, ЦРУ, АНБ з іноземними спецслужбами до створення системи автоматичного обміну інформацією, а також організація особливої оперативної групи з кібербезпеки у Стратегічному командуванні США; 3) кібернетична підтримка військових операцій США й залучення кваліфікованих цивільних фахівців [11; 15].

У лютому 2016 р., відкриваючи в Таллінні дводенну конференцію "EU global strategy for Foreign and Security Policy", організовану Міністерством оборони Республіки Естонія та Естонським міжнародним центром оборонних досліджень, Міністр закордонних справ Естонії Марина Кальюран відмітила необхідність більш реалістично відображати у глобальній стратегії зовнішньої політики й політики безпеки ЄС ситуацію щодо кібербезпеки та необхідність встановлення всесвітніх норм кібербезпеки [11; 16].

На початку квітня 2016 р., виступаючи у Брюсселі на третьому семінарі зі співробітництва ЄС і НАТО в галузі кібербезпеки, міністр висловила думку, що кібератаки - своєрідна норма сучасних міжнародних відносин. "Ми вважаємо за необхідне підвищити політичне й оперативне співробітництво в галузі кібероборони й обмін інформацією між ЄС і НАТО. Більш широкий підхід ЄС до кібербезпеки та сфокусована на кібероборонні діяльність НАТО взаємно доповнюються. Обмін інформацією дозволяє ефективніше виявляти всі інциденти і швидше на них реагувати," - заявила міністр. Вона вказала на необхідність розвивати навички в цій сфері і планувати спільні навчання [11; 17].

Щодо Литовської Республіки, то, за даними CERT-LT, у 2011 р. у Литві було проведено розслідування з приводу 21,8 тис. повідомлень про події в електронному просторі. Цього ж року було затверджено Програму розвитку електронної інформаційної безпеки на 2011-2019 рр.

У грудні 2014 р. сейм Литви прийняв Закон "Про кібернетичну безпеку". Несподіванкою стала закладена у ньому норма: інтернет-провайдер може припинити надання послуг особам, якщо їхня діяльність суперечить інформаційній безпеці держави. Також за Законом 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 [18].

У 2016 р. було затверджено нову редакцію Воєнної стратегії Республіки Литва (The military strategy of the republik of Litvinia), у якій відображена реакція держави на нові тенденції як у політиці, так і у вирішенні конфліктів. Якщо в першій Доктрині (2010 р.) йшлося тільки про заходи з індивідуальної оборони країни, то в новому документі передбачено дії як з індивідуальної оборони, так і з колективної, із урахуванням членства Литви в Північноатлантичному Альянсі. Важливе місце посідає опис викликів, які постали перед НАТО та Європейським Союзом через агресивну політику Росії, а також необхідну реакцію на них [19].

У 2017 р. сейм Литви затвердив нову Стратегію національної безпеки країни (National Security Strategy), у якій визначено широкий спектр актуальних для країни загроз: глобальна економічна криза, виклики кібернетичній та інформаційній безпеці, конвенційна загроза з боку РФ тощо. Зокрема, за Стратегією, до інформаційних загроз належать:

- військова пропаганда, поширена певними державами;

- підбурювання до ненависті, спроби спотворити історію та інша необґрунтована та викривлена інформація, спрямована проти інтересів національної безпеки держави, що веде до недовіри та незадоволеності, спроби дискредитувати членство Литви в НАТО, можливості НАТО і зобов'язання захищати союзників, інформаційні заходи, спрямовані впливати на демократичні або виборчі процеси у країні. До кібернетичних загроз належать напади на об'єкти критичної інфраструктури [Там само].

З 1 січня 2018 р. у Литві планується функціонування нової системи національної кібернетичної безпеки. Свою роботу розпочинає служба інформаційної безпеки, у планах - створення трьох киберпідрозділів (модулів кібернетичної оборони та управління мережами чисельністю 20 фахівців), підпорядкованих Міністерству оборони. Перший модуль - постійної бойової готовності - буде складатися з професійних військовослужбовців, тоді як два інших складатимуться з резервістів, які за потреби будуть включені в загальну діяльність.

У Латвії державне управління, суспільство й економіка цілком залежать від послуг і можливостей, що надаються інформаційно-комунікаційними технологіями. Як свідчать результати соціологічних опитувань, більш ніж 70 % мешканців країни регулярно користуються комп'ютером і послугами Інтернету [Там само].

У 2011 р. у Латвії було прийнято Закон "Про безпеку інформаційних технологій". Відповідно до нього створено Раду з безпеки інформаційних технологій, на яку покладено обов'язки 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 [19].

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 [18].

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 [2].

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 ме-

тою 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 [20].

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" [21].

22 січня 2014 р. на засіданні Кабінету міністрів були затверджені основні положення латвійської Стратегії кібербезпеки на 2014-2018 рр. та План дій щодо її виконання, підготовлені Міністерством оборони. Документ характеризує ситуацію кібербезпеки в Латвії та існуючі проблеми, а також визначає основні принципи формування політики кібербезпеки, мету й пріоритетні напрямки подальших дій [19].

За Стратегією, метою політики кібербезпеки Латвії є безпечне й надійне кіберсередовище, у межах якого гарантовано безперервне, надійне й безпечне отримання послуг, важливих для держави та суспільства. Для здійснення поставленої мети визначені три напрямки діяльності: управління кібербезпекою і ресурсами, правопорядок у кіберпросторі і зниження рівня кіберзлочинності, розуміння в суспільстві, освіта й дослідницька робота, а також готовність і спроможність у кризових ситуаціях і міжнародне співробітництво [22].

У 2015 р. у Республіці прийнято Концепцію національної безпеки. Головною небезпекою в медіапросторі Латвії вважають російську медіаполітику [3].

Останнім часом значно активізовано роботу Центру стратегічних комунікацій НАТО, створеного влітку 2015 р., який відповідає за стратегічні комунікації Альянсу. Місія Центру полягає у проведенні досліджень і розробці рекомендацій щодо ведення інформаційних і психологічних операцій, а також щодо суспільних відносин, пропаганди.

Проте в Латвії, як і в інших прибалтійських країнах, спостерігається брак фахівців з інформаційних технологій, незважаючи на щорічну підготовку близько тисячі ІТ-спеціалістів. В академічні програми підготовки впроваджено також курс з інформаційної безпеки.

Висновки

Аналіз діяльності у сфері забезпечення інформаційної безпеки країн Балтії дає підстави сформулювати висновки.

1. Особливістю забезпечення інформаційної безпеки у країнах Балтії є зосередження уваги державних органів на питаннях, пов'язаних із кібернетичною безпекою. Це пояснюється передусім високим рівнем інформатизації в цих країнах та членством останніх у ЄС та НАТО.

2. Зміст керівних документів з питань забезпечення кібербезпеки прибалтійських країн відповідає вимогам керівних документів НАТО у цій сфері, яка передбачає діяльність у трьох напрямах: захист власної інфраструктури від хакерських атак; міжнародну співпрацю в цій галузі та залучення цивільних фахівців. У країнах Балтії ми спостерігаємо реалізацію всіх зазначених напрямів. Окремо слід відзначити створення кібернетичних центрів НАТО на території країн Балтії із відповідною спеціалізацією.

3. Цікавим та інформативним є факт залучення до співпраці та захисту кіберпростору країн Балтії працівників приватного сектора та кіберволонтерів і закріплення їхніх повноважень на законодавчому рівні. Для нашої країни факт залучення фахівців з інформаційних технологій для спільної роботи з державними інституціями є позитивним і корисним, необхідним для впровадження, ураховуючи той факт, що під час російської гібридної агресії щодо України сформувались спільноти "інфоволонтерів - загальновідомі Inform Napalm, StopFake, "Информационное сопротивление" тощо.

ЛІТЕРАТУРА

1. Гапеєва О. Л. Історико-ментальні складові конфліктності в інформаційній сфері між Росією та країнами Балтії / О. Л. Гапеєва // Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. - Серія Історія. Вип. 1, ч. 2. - 2017. - С. 60-65.

2. 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.

3. Drošī bas policija [Електронный ресурс]. - Режим доступу : http://dp.gov.lv/lv/noderigi/publikacijas.

4. International Security and Estonia: report [Електронный ресурс]. - Режим доступу : https://www.teabeamet.ee/pdf/EIB_public_report_Feb_2017.pdf.

5. Estonian Cyber Security Strategy for the year 2008-2013 to be presented [Електронний ресурс]. - Режим доступу : http://www.baltic-course.com/eng/Technology/?doc=1952.

6. Правительство Эстонии утвердило стратегию кибербезопасности страны [Електронний ресурс]. - Режим доступу : https://www.kp.ru/online/news/86868/.

7. Information System Authority [Електронний ресурс]. - Режим доступу : https://www.ria.ee/en/about-estonian-information-system-authority.html.

8. Information Technology Foundation for Education [Електронний ресурс]. - Режим доступу: http://www.hitsa.ee/about-us.

9. Critical Information Infrastructure Protection [Електронний ресурс]. - Режим доступу : https://www.ria.ee/en/ciip.html.

10. History of the EDL CU [Електронний ресурс]. - Режим доступу : http://www.kaitseliit.ee/en/history-of-the-edl-cu.

11. Кибернетический бастион НАТО в Прибалтике в действии [Електронний ресурс]. - Режим доступу : https://www.ritmeurasia.org/news--2016-11-20--kiberneticheskij-bastion-nato-v-pribaltike-v-dejstvii-26949.

12. Эстония модернизирует крупнейший в Европе киберполигон [Електронний ресурс]. - Режим доступу : https://www.ria.ee/en/about-estonian-information-system-authority.html.

13. Cyber Security Strategy [Електронний ресурс]. - Режим доступу : https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

14. Учения киберзащитников "Cyber Coalition 2015" [Електронний ресурс]. - Режим доступу : http://www.melkon.lv/news/2015/11/19/ucheniya-kiberzashhitnikov-cyber-coalition-2015/.

15. Селянин Я. В. Роль Пентагона в обеспечении кибербезопасности США / Я. В. Селянин // Проблемы национальной стратегии. - М. : PICI, 2017. - № 3 (42). - С. 130-147.

16. В Таллине обсуждают проблемы европейской кибербезопасности [Електронний ресурс]. - Режим доступу : https://www.tatar-inform.ru/news/2016/02/04/490207/.

17. Глава эстонского МИДа призвала ЕС и НАТО укрепить кибероборону [Електронний ресурс]. - Режим доступу : http://baltnews.ee/policy/20160407/1014657973.html.

18. Кибернетическая безопасность: ситуация в Литве и странах Балтии [Електронний ресурс]. - Режим доступу :

https://net-artis.com/kiberneticheskaya-bezopasnost-situaciya-v-litve-i-stranax-baltii/]

19. 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.

20. Zemessardzes Kiberaizsardzī bas vienī ba [Електронний ресурс]. - Режим доступу : http://www.zs.mil.lv/Zemessardzes%20vienibas/kiberaizsardzibas_vieniba.aspx.

21. Nacionālo bruņoto spēku 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.

22. Nacionālās drošī bas koncepcija (informatī vā daļ a) [Електронний ресурс]. - Режим доступу : https://likumi.lv/ta/id/278107-par-nacionalas-drosibas-koncepcijas-apstiprinasanu.

Гапеева Ольга,
кандидат исторических наук, старший научный сотрудник, докторант,
Национальная академия сухопутных войск имени гетьмана Петра Сагайдачного, г. Львов

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ В СТРАНАХ БАЛТИИ: ИСТОРИЧЕСКАЯ РЕТРОСПЕКТИВА

В статье рассматриваются особенности становления национальных систем обеспечения кибернетической безопасности стран Балтии в исторической ретроспективе с учетом положений документов Европейского Союза и НАТО в этой сфере. Хронологические рамки исследования охватывают период с 2004 по 2016 год.

Показано, что страны Балтии долгое время находятся в эпицентре кибернетических и информационных атак со стороны Российской Федерации. Об этом свидетельствует содержательный анализ русскоязычного контента в информационном пространстве прибалтийских стран и отчетный материал спецслужб Латвии, Литвы и Эстонии, размещенный на официальных web-сайтах этих учреждений.

Ключевые слова: *информационная безопасность; информационная угроза; кибербезопасность; киберстратегия; национальная безопасность; страны Балтии.*

Gapeyeva Olga,
Candidate of Historical Sciences, Senior Researcher Doctorate student,
Lviv National military Academy named after hetman Sagaydachny

PECULIARITIES OF CYBER SECURITY IN THE BALTIC STATES: HISTORICAL RETROSPECTIVE

The Russian Federation conducts an information policy in the Baltic direction, aimed at forming a negative image of Latvia, Lithuania and Estonia in the international scene through involving research and development institutions, Russian media and social networks to informational propaganda. Main forms and methods of destructive influence on Russian-speaking population of the Baltic countries have been identified in previous studies.

So, the Baltic countries for a long time are in the epicentre of cyber and information attacks by Russian Federation.

The aim of the study is to analyze the activities of the Latvia, Lithuania and Estonia of formation of national systems for ensuring cyber security in historical retroperspective, the provisions of the documents of the European Union and NATO in this area. The article is based on the documentary sources from 2004 to 2016.

The contents of the guidance documents on issues of cyber security of the Baltic countries meets the requirements of the governing documents of NATO in this sphere and involves activities in three directions: protecting its own infrastructure from hacker attacks; international cooperation in this sphere and the involvement of civil experts. That is we can see implementation of all these directions in the Baltic countries.

Feature of information security in the Baltic States is focusing on issues related to cyber security. This is primarily due to high level of Informatization in there countries and their membership in European Union and NATO.

Key words: *information security; information risk; cyber security; cyber strategy; national security; the Baltic States.*

REFERENCES

1. Gapeyeva, O. L. (2017), Informational confrontation between Russia and Estonia on the example of «Bronze Night» events on 2007, *Military Historical Meridian*, Kyiv, Vol.15, available at: http://vim.gov.ua/images/sbor/VIM_15_2017-86-98.pdf (ukr).

2. Gapeyeva, O. L. (2017), Historical-mental conflict prerequisites in the informational sphere between Russia and Baltic states, *Scientific notes of Ternopil Volodymyr Hnatiuk National Pedagogical University*, Ternopil, Vol.1, part 2, pp.60-65 (ukr).

3. Drošī bas policija, available at: http://dp.gov.lv/lv/noderigi/publikacijas (lat).

4. International Security and Estonia: report, available at: https://www.teabeamet.ee/pdf/EIB_public_report_Feb_2017.pdf (eng).

5. Estonian Cyber Security Strategy for the year 2008-2013 to be presented, available at: http://www.baltic-course.com/eng/Technology/?doc=1952 (eng).

6. The Estonian government adopted the cybersecurity strategy of the country, available at: https://www.kp.ru/online/news/86868/ (rus).

7. Information System Authority, available at: https://www.ria.ee/en/about-estonian-information-system-authority.html (eng).

8. Information Technology Foundation for Education, available at:http://www.hitsa.ee/about-us (eng).

9. Critical Information Infrastructure Protection, available at: https://www.ria.ee/en/ciip.html (eng).

10. History of the EDL CU, available at: http://www.kaitseliit.ee/en/history-of-the-edl-cu (eng).

11. The cybernetic bastion of NATO in the Baltics in action, available at: https://www.ritmeurasia.org/news—2016-11-20—kiberneticheskij-bastion-nato-v-pribaltike-v-dejstvii-26949 (rus).

12. The internal security. Official website of the Ministry of internal Affairs of Estonia, available at: https://www.siseministeerium.ee/ru/vnutrennyaya-bezopasnost/obespechenie-vnutrenney-bezopasnosti (rus).

13. Estonia is modernising Europe's largest cyber range, available at: https://www.ria.ee/en/about-estonian-information-system-authority.html (eng).

14. Cyber Security Strategy, available at: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf/ (rus).
15. The teachings of cybersemiotics «Cyber Coalition 2015», available at: https://www.melkon.lv/news/2015/11/19/ucheniya-kiberzashhitnikov-cyber-coalition-2015/ (rus).
16. Seljanin, Ja. V. (2017), The role of the Pentagon in cybersecurity USA, *National security issues*, Vol.3(42), pp.130-147 (rus).
17. In Tallinn to discuss European cyber-security, available at: https://www.tatar-inform.ru/news/2016/02/04/490207/ (rus).
18. The head of the Estonian foreign Ministry called on the EU and NATO to strengthen the cyber defence, available at: http://baltnews.ee/policy/20160407/1014657973.htm/ (rus).
19. Cyber security strategy of Latvia 2014-2018, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (eng).
20. Zemessardzes Kiberaizsardzī bas vienī ba, available at: http://www.zs.mil.lv/Zemessardzes%20vienibas/kiberaizsardzibas_vieniba.aspx (lat).
21. Nacionālo bruņoto spēku kiberaizsadzī bas vienī bas (kav) koncepcija, available at: http://www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/%20cyberzs_April_2013.ashx (lat).
22. Nacionālās drošī bas koncepcija (informatī vā daļ a), available at: https://likumi.lv/ta/id/278107-par-nacionalas-drosibas-koncepcijas-apstiprinasanu (lat).

Надійшла до редакції 13.11.2017

УДК [327.7 (477): 430] "1918/1923)
DOI: 10.21847/1728-9343.2017.6(152).122285

ЗАБОЛОТНЮК ВОЛОДИМИР,
здобувач, провідний науковий співробітник
Науково-дослідного відділу (механізованих і танкових військ),
Науковий центр Національної академії сухопутних військ, м. Львів

УКРАЇНСЬКІ ДИПЛОМАТИЧНІ ІНСТИТУЦІЇ В НІМЕЧЧИНІ В 1918-1923 рр.

У статті розглядається становлення та діяльність у Німеччині українських посольств та консульських установ у 1918-1923 рр. У Берліні були представлені дипломатичні установи Української Народної Республіки доби Центральної Ради (посол Олександр Севрюк), Української Держави (барон Федір Штейнґель), Української Народної Республіки доби Директорії УНР (Микола Порш, Роман Смаль-Стоцький). Своє посольство утворила в Берліні й Західно-Українська Народна Республіка (Євген Левицький, Ярослав Біберович). Але з огляду на можливу негативну реакцію країн Антанти посольство ЗУНР не розвинуло ширшої діяльності. Україна мала свої консульські установи в Берліні та Мюнхені. У статті згадується також про діяльність української консульської установи в Данцигу (Гданську), який був тісно пов'язаний з Німеччиною. Українські дипломатичні структури в Німеччині були офіційно визнані німецькою владою й свої головні зусилля спрямували на пошуки зовнішньої підтримки України в боротьбі з ворогами її незалежності. Дипломати разом із військово-санітарними місіями здійснювали опіку над полоненими українцями - вояками колишньої російської армії, які утримувалися в таборах Німеччини, також піклувалися про тих українців, які залишилися в еміграції й працювали чи навчалися в цій країні.

Ключові слова: *дипломатія; посольства; консульські установи; військова еміграція; Ярослав Біберович; Євген Левицький; Микола Порш; Олександр Севрюк; Роман Смаль-Стоцький; Федір Штейнгель.*

Постановка та актуальність проблеми. Українські національні уряди в добу революції за кордоном створювали дипломатичні установи та місії. Їхня діяльність мала серйозний вплив на міжнародний аспект самостійницьких прагнень українських урядів. Українська дипломатія новітнього характеру відзначає 100-літній ювілей.

На окремий розгляд заслуговує діяльність українських дипломатів у 1918-1923 рр. у Німеччині, яка офіційно визнала українську державність. Відтак вивчення становлення та діяльності українських дипломатичних установ у Німеччині сприятиме глибшому розумінню міжнародного контексту українських визвольних змагань та обставин становлення української військової еміграції.