УДК: [32:004.56](474) *© Оксана Звоздецька*

КІБЕРБЕЗПЕКА КРАЇН БАЛТІЇ: СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ[1]

Стаття присвячена аналізу правових та інституційних механізмів забезпечення кібернетичної безпеки країнами Балтії в умовах сучасних викликів і загроз міжнародній безпеці. Серед них найбільше занепокоєння викликають зростаючі масштаби інформаційного тероризму, кібератак, кіберзлочинності, зростаюча агресивність зовнішньої політики Росії, та ведення нею асиметричних війн.

В дослідженні охарактеризовано кібербезпекові стратегії Естонії, Литви та Латвії, діяльність відповідальних органів, а також спільні дії цих країн щодо зміцнення захисту кіберпростору регіону.

Ключові слова: *кіберпростір, кібератаки, кібербезпека, країни Балтії.*

Кибербезопасность стран Балтии: современные вызовы и угрозы

Статья посвящена анализу правовых и институциональных механизмов обеспечения кибернетической безопасности странами Балтии в условиях современных вызовов и угроз международной безопасности. Среди них наибольшее беспокойство вызывают растущие масштабы информационного терроризма, кибератак, киберпреступности, растущая агрессивность внешней политики России, и ведения ею асимметричных войн.

В исследовании охарактеризованы стратегии кибербезопасности Эстонии, Литвы и Латвии, деятельность ответственных органов, а также совместные действия этих стран по укреплению защиты киберпространства региона.

Ключевые слова: *киберпространство, кибератаки, кибербезопасность, страны Балтии.*

Baltic cybersecurity: new challenges and threats

The body of the article goes on to discuss effective legal and institutional framework to ensure and strengthen cyber security in the Baltic region with

[1] ***Для цитування:*** Звоздецька О. Кібербезпека країн Балтії: сучасні виклики та загрози // Медіафорум : аналітика, прогнози, інформаційний менеджмент: збірка наукових праць. Чернівці: Чернівецький національний університет, 2017. Том 5. С. 20-34.

regard to modern challenges, threats and vulnerability of the international security. Noteworthy, the potential threats posed by cyber terrorism, cyber attacks, cyber-crime are daunting, as well as Russia's pushing its foreign policy in increasingly aggressive ways and its asymmetric warfare.

The study described cyber security strategy of Estonia, Latvia and Lithuania, delves into responsible authorities performing their functions, as well as joint efforts of these countries to enhance and strengthen protection of cyberspace region.

Keywords: *cyberspace, cyber attacks, cyber security, the Baltic countries.*

Постановка проблеми. Еволюція і широкий доступ до інформаційних технологій надають нові можливості для маніпулювання і задоволення нездорових амбіцій. Зростає кількість політично мотивованих кібернетичних інцидентів, спрямованих проти безпеки держав, включаючи їх збройні сили. Колишній Президент Естонії Тоомас Хендрик Ільвес підкреслив, що «кібербезпека не знає географії, і ми не можемо вирішити цю проблему поодинці» [17, с. 63].

Виокремлюють три ключові чинники, що вимагають покращення кібербезпеки у глобальному масштабі. Повсюдна широкосмугова мережа, бізнес і суспільство, орієнтовані на інформаційні технології (ІТ), та соціальна стратифікація навичок використання ІТ змінюють традиційне середовище ІТ з централізованим контролем та управлінням на відкритий світ, де всі користуються багатьма пристроями, із розмитими межами між діловим та особистим. Водночас багато ділових операцій уже позбавлені нецифрових (паперових або очних) альтернатив. Такі зміни супроводжуються появою на світовому ринку нового покоління користувачів та пристроїв. Це нове покоління має кардинально інше бачення безпеки і більш схильне до переважаючої довіри та розповсюдження ідей в чисельних соціальних мережах, платформах для обміну та наданні інноваційних послуг.

На Думку Директора Центру передових технологій з кібероборони НАТО Полковника Ільмара Тамма, для забезпечення ефективної кібернетичної оборони необхідно завжди бути в курсі щодо рівня реальної загрози і небезпеки, тобто того, що військові називають «загальною оперативною картиною», так само як і підтримувати здатність визначати тенденції на підставі досвіду і спостережень. Отже, навіть теоретично, підготовка оборони проти кібернетичного нападу є найбільш складним завданням[27, с. 8].

Для боротьби з кіберзлочинністю та кібератаками багато урядів та установ запустили ініціативи в галузі кібербезпеки, починаючи з настанов і стандартизації та закінчуючи комплексним законодавством і регуляторними актами [1].

Інформаційна та гібридна війна РФ проти України привернула увагу всіх країн, але особливий інтерес вона викликала у країн Східної Європи, оскільки вони виразно відчувають таку ж вразливість до зовнішніх дій у власних фізичному, інформаційному та віртуальному просторах. Особливу увагу на цю ситуацію звернули всі сусіди Росії: Латвія, Литва, Естонія, Польща, а також Білорусія і Казахстан. Тому, на сьогодні є актуальним та необхідним для України вивчення досвіду країн Балтії в сфері кібербезпеки.

Аналіз останніх досліджень і публікацій. Проблематика статті частково досліджувалась в роботах таких вітчизняних науковців як О. Запорожець [25], М. Замікула [24] та А. Баровська [19], які розглядають політику ЄС та НАТО в сфері інформаційної безпеки.

Мета статті. Проаналізувати правові та інституційні аспекти захисту кіберпростору Естонією, Латвією та Литвою, а також спільні кроки для зміцнення регіональної кібербезпеки.

Виклад основного матеріалу. Рівень участі держав у сфері кібербезпеки дозволяє оцінити Глобальний індекс кібербезпеки (ГІК (Global Cybersecurity Index)), який є дітищем колективного партнерства між ABI Research[1] і Міжнародним союзом електрозв'язку (МСЕ), і спрямований на те, щоб вивести питання кібербезпеки в число пріоритетів національних стратегій різних країн.

Індекс був повністю визнаний на Повноважній конференції МСЕ в Пусані і включений до Резолюції 130 (Ред. Пусан, 2014 г.) «Посилення ролі МСЕ в зміцненні довіри і безпеки при використанні інформаційно-комунікаційних технологій». Зокрема, Державам-членам запропоновано «підтримати ініціативи МСЕ в сфері забезпечення кібербезпеки, в тому числі за допомогою використання Глобального індексу кібербезпеки (ГІК), з метою заохочення стратегій урядів і спільного використання інформації про діяльність в різних галузях і секторах» [4, с. 254].

[1] ABI Research – це компанія, що займається дослідженням ринку, зокрема, глобальних ринків технологій, методами складання кількісних прогнозів і аналізу найважливіших показників і тенденцій.

Створений на основі Глобальної програми кібербезпеки МСЕ [2], ГІК оцінює рівень зобов'язань в п'яти сферах: правові, технічні, організаційні заходи, розвиток потенціалу та міжнародне співробітництво. Результатом став індекс на рівні окремих країн і глобальний рейтинг готовності системи кібербезпеки.

Метою ГІК є створення загальної картини того на якому рівні знаходяться країни в справі забезпечення національної кібербезпеки. Над проектом ГІК з 2014 р. працювали Бюро розвитку електрозвязку (БРЕ), зокрема, Відділ кібербезпеки і додатків ІКТ (CYB), і ABI Research. CYB виступав в якості координатора і власника проекту, а ABI Research використовував свої експертні знання для розробки стратегії, аналізу діяльності конкурентів, планування бізнесу, оцінки технологій і галузевого порівняльного аналізу в процесі реалізації проекту. Естонія за даними цього звіту знаходиться на 5 місці в глобальному рейтингу, поряд з такими країнами як Німеччина, Японія, Великобританія та Індія. Латвія разом з Туреччиною та Швецією оцінюється в 7 балів; Литва – 14 балів – на рівні Китаю, Бельгії, Нігерії, Судану [3, с. 1-2].

Отже, найбільш розвиненою і захищеною серед країн Балтії є Естонія, яка за 2016 р. визнана країною з найбільш вільною економікою ЄС, і шоста в цій номінації в світі. Естонія – це держава з найнижчим державним боргом в Європі, і збалансованим державним бюджетом, стала першою державою в світі, яка просуває ідею світу без кордонів, зокрема, в 2014 р. ввела е-громадянство (e-residency). Країна з розвиненим е-урядуванням, в якій громадяни отримують більше 3300 послуг, що надаються державою, перша в світі за кількістю стартапів в перерахунку на душу населення [18, с.58-59].

Для посилення кібербезпеки 8 травня 2008 р. урядом Естонії затверджено «Стратегію кібербезпеки на 2008-2013 рр.» [10]. Стратегічними цілями Естонії у сфері кібербезпеки є створення багаторівневої системи безпекових заходів; розширення компетенції та обізнаності громадян країни з питань інформаційної безпеки; правове регулювання питань кібербезпеки; зміцнення позиції Естонії як однієї з країн-лідерів у міжнародній співпраці в сфері кібербезпеки. При створенні багаторівневої системи безпекових заходів пріоритетне значення надається захисту критичної інформаційної інфраструктури, розробці і впровадженню заходів безпеки та організаційному співробітництву.

Для зміцнення організаційного співробітництва передбачено реалізацію таких заходів, як створення Ради з кібербезпеки у Комітеті з питань безпеки естонського уряду, уповноваженого втілювати у життя Стратегію кібербезпеки; визначення повноважень структурного підрозділу Міністерства економіки і комунікацій, що відповідає за безпеку державних інформаційних систем; вдосконалення методів оцінки ризиків, розроблених міністерствами та використання цих методів в сфері кібербезпеки; створення експертної робочої групи, уповноваженої виявляти прогалини в інформаційній безпеці, визначати необхідні ресурси для оновлення безпекових заходів та обмінюватися оперативною інформацією тощо [10].

В 2014 р. прийнято новий документ «Стратегію кібербезпеки на 2014-2017 рр.» [8]. Ця стратегія продовжує реалізацію багатьох цілей, покладених в Стратегію 2008 р., проте, була доповнена сучасними загрозами та потребами, які не були охоплені попереднім документом.

Чотирирічна мета стратегії кібербезпеки полягає в збільшенні можливостей в сфері кібербезпеки і підвищення рівня поінформованості населення про кіберзагрози, забезпечуючи тим самим безпеку кіберпростору. Загальна вартість реалізації заходів, передбачених в стратегії приблизно була оцінена в 16 млн. євро [11, с.18].

Основними способами підвищення компетентності в сфері кібербезпеки визначено організацію навчань (тренінгів) з питань кібербезпеки та проведення досліджень. Сюди відноситься, зокрема, встановлення вимог до знань у сфері інформаційної безпеки та кіберзахисту для робітників державного і приватного секторів та впровадження відповідної системи оцінювання; підвищення рівня підготовленості до кризових ситуацій у державному та приватному секторах тощо.

Розробка і впровадження політики інформаційної безпеки належить до компетенції Міністерства економіки та комунікацій, а точніше таких його структурних підрозділів, як Департамент державної інформаційної системи [29] та Естонський центр інформатики.

З 1 червня 2011 р. Естонський центр інформатики був реорганізований в Управління інформаційної системи Естонії (Estonian Information System's Authority (EISA)) [30], яке допомагає організаціям приватного та державного сектору підтримати безпеку своїх інформаційних систем та захистити критичні інфраструктури; цей орган має також право нагляду.

Управління інформаційної системи Естонії включає в себе ряд підрозділів, які комплексно забезпечують кібербезпеку країни. Зокрема, Департамент з захисту критичних інформаційних інфраструктур (Critical Information Infrastructure Protection CIIP), Центр обміну документами (About document exchange centre (DEC)), - інформаційна система, що забезпечує загальну центральну службу обміну документами для різних систем управління документами (DMS), Інфраструктура відкритих ключів (Public Key Infrastructure PKI), що забезпечує безпечну цифрову аутентифікацію і цифрові підписи, IT-інфраструктура (IT Infrastructure) забезпечує, щоби основні інформаційні послуги держави були доступні навіть в разі форс-мажору.

З 2006 року в Естонії працює Комп'ютерна група швидкого реагування (CERT Estonia) – організація, відповідальна за управління безпековими інцидентами у комп'ютерних мережах домену «.ee». Комп'ютерною групою швидкого реагування Естонії надаються такі послуги: прийняття повідомлень про інцидент; аналіз інциденту; надання допомоги у реагуванні на інцидент; координація дій з реагування на інцидент; інформування Інтернет-користувачів про атаки, віруси, «хробаків», «троянів» в мережах домену першого рівня «.ee» та сповіщення про вразливі місця, виявлені у найбільш популярних в Естонії системах і додатках. В країні також функціонує декілька неурядових організацій, які роблять свій внесок у зміцнення інформаційної безпеки держави [5].

Окрім цього, у Брюсселі 14 травня 2008 р. був підписаний меморандум про створення в Естонії (м. Таллінн) міжнародного Центру передових технологій з кібероборони НАТО, з розташуванням його штаб-квартири у Таллінні і надання йому статусу міжнародної військової організації. Завдяки його потужностям Естонія стала однією з найбільш захищених від кібератак країною в ЄС. У сучасних умовах у роботі вказаного центру беруть участь 16 європейських країн.

Фінансування Центру здійснює не власне НАТО, а лише окремі держави-члени Альянсу, які є спонсорами проекту та учасниками його діяльності. Естонська Республіка, як держава, на території якої розташований Центр, фінансово забезпечує його інфраструктуру та адміністративні витрати, у той час як інші країни-учасники відповідають за заробітну платню та витрати на проживання власних експертів та роблять внески у спільний бюджет Центру. Також Центр відкритий для налагодження партнерських відносин з державами,

які співпрацюють з Альянсом, вищими навчальними закладами та дослідницькими інститутами, але такі партнери не користуються правами націй-спонсорів та, звичайно, не мають права голосу у керівних органах Центру. Робота центру поділяється на три напрямки: право і принципи, технології та стратегія [24, с. 57].

Основоположними документами, що визначають політику Латвії у сфері кібербезпеки, є Концепція національної безпеки 2011 р. та Стратегія кібербезпеки Латвії 2014-2018 рр. [9]. В Стратегії зазначається, що при реалізації політики кібербезпеки, використовуються наступні принципи – розвиток, співпраця, відповідальність і відкритість. Сучасне суспільство використовує ІКТ більш широко ніж отримання інформації та її обробка і створює нові і широкодоступні інструменти для самовираження, зручні і різноманітні засоби спілкування та платформи, що використовуються для отримання послуг. В цілому 75,8% жителів Латвії користуються Інтернетом, кількість електронних угод в найбільших банках Латвії перевищує 90% від загальної кількості угод, і більше 25% послуг державних установ доступні в електронному вигляді [9]. В Стратегіїі для визначення кібербезпеки наводиться поняття, що було сформульовано в Рекомендації Міжнародного союз електрозв'язку МСЕ-Т Х.1205, яка була прийнята у 2010 р.: «Кібербезпека це набір засобів, стратегій, принципів забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберсередовища (кіберпростору) [9].

Для того, щоб зменшити кількість випадків, коли за допомогою ІКТ суспільству наносять значні збитки, було визначено пріоритетні напрямки діяльності, які будуть захищати кіберпростір, зокрема:управління та ресурси комп'ютерної безпеки, верховенство закону в кіберпросторі і скорочення кіберзлочинності, антикризове управління, підвищення поінформованості суспільства про кіберризики та загрози, освіта і наукові дослідження.

Національну політику в сфері кібербезпеки забезпечують:

1. Міністерство оборони (МО), що координує розробку і впровадження інформаційних технологій політику безпеки і захисту інформаційних систем, а також забезпечує міжнародне співробітництво.

2. Міністерство внутрішніх справ (МВС), Державна поліція (ДП) і Поліція безпеки (SeP) – здійснюють політику в сфері боротьби зі

злочинністю, охорони громадського порядку, забезпечення безпеки, а також захист прав і законних інтересів осіб, а також координує врегулювання кризових ситуацій.

3. Латвійський Центр з протидії кіберзагрозам (CERT.LV) здійснює моніторинг і аналіз подій в кіберпросторі, реагує на кіберінциденти, здійснює їх координацію та профілактику, проводить дослідження, організовує освітні заходи та навчання. CERT.LV відповідає за безпеку у всьому латвійському електронному інформаційному просторі.

Перша Команда реагування на кіберінциденти (LATNET CERT) була заснована ще в 2006 році і, на її основі в 2011 р. було створено Латвійський Центр з протидії кіберзагрозам (CERT.LV), що працює при Міністерстві оборони Латвійської Республіки і регулюється Законом «Про безпеку інформаційних технологій» [6].

4. Центр з забезпечення безпечного Інтернету в Латвії (Operation of the Safer Internet Centre of Latvia NetSafe) – інформує суспільство про можливі ризики і загрози онлайн, сприяє використанню безпечного Інтернет-контенту.

5. Національні збройні сили і кібернетичної оборони (Unit National Armed Forces (NAF) and Cyber Defence Unit (CDU)) – надають підтримку в кризових ситуаціях.

Ще в 2012 р. Латвія заявила про свій намір створити спеціалізований центр НАТО з стратегічних комунікацій. На офіційному рівні Альянсу було визнано, що саме в контексті російської агресії проти України діяльність Центру є життєво необхідною для посилення відповідної спроможності НАТО. 1 липня 2014 р. в Командуванні НАТО в Норфолку (США) Латвія, Естонія, Італія, Литва, Польща, Великобританія і Німеччина - підписали меморандуми про створення в Ризі міжнародного Центру стратегічних комунікацій. Центр працює як центральний осередок для обговорення та експертизи різних дисциплін зі сфери стратегічних комунікацій: публічної дипломатії, зв'язків із громадськістю, військових зв'язків із громадськістю, контр-пропаганди, інформаційних і психологічних операцій [19, с. 148]. Необхідно відзначити, що таких центрів у державах Альянсу двадцять, три з яких розташовані у державах Балтії: Естонія (кібербезпека), Литва (енергетична безпека), Латвія (стратегічні комунікації).

Рада НАТО акредитувала центр 1 вересня [21]. На заснування Центру було виділено 2,7 мільйона євро. На 2015 р. бюджет Центру

було затверджено у розмірі 505,250 євро. У 2015 р. Центр отримав 999,985 доларів як особливий внесок з боку канадського уряду для підтримки зусиль Центру щодо вдосконалення своїх стратегічних комунікаційних можливостей [14, с. 18].

20 серпня 2015 р. в Ризі відкрився новий офіс Центру стратегічних комунікацій НАТО (Stratcom). На урочистій церемонії були присутні президенти Латвії Раймондс Вейоніс, котрий сказав, що якщо в 2012 р. поняття стратегічної комунікації було чимось далеким, та в наші дні воно стало реальністю. Президент підкреслив роль стратегічної комунікації в сучасну епоху інформаційних та гібридних воєн. «Кожен день йде боротьба за уми і серця людей», – сказав Р.Вейоніс, додавши, що сьогодні ми повинні бути готові до будь-якої ситуації, і значення стратегічної комунікації з кожним днем зростає [26].

Завданнями Центру є:

• розроблення програм для сприяння розвитку та гармонізації доктрини стратегічних комунікацій;

• проведення досліджень та експериментів з метою пошуку практичних рішень для розв'язання існуючих проблем;

• «вивчення уроків» застосування стратегічних комунікацій під час військових операцій;

• підвищення навчальних та освітніх зусиль і можливостей взаємодії [15].

На сьогодні Центр визначає стратегічні комунікації, як «скоординоване і належне використання комунікативної діяльності і можливостей НАТО з метою підтримки політики, операцій і діяльності Альянсу, а також в цілях просування цілей НАТО. Цією діяльністю та можливостями є: публічна дипломатія, зв'язки із громадськістю, військові зв'язки із громадськістю, інформаційні операції та психологічні операції» [13].

Документами, що забезпечують кібербезпеку Литовської Республіки є «Програма розвитку електронної інформаційної безпеки (кібербезпека) на 2011-2019 рр.», що була затверджена урядом 29 червня 2011 р. Мета Програми полягає у визначенні цілей і завдань для розвитку електронної інформації з метою забезпечення конфіденційності, цілісності та доступності електронної інформації та послуг, що надаються в кіберпросторі, охорони електронних комунікаційних мереж, інформаційних систем і критично важливих інформаційних інфраструктур від інцидентів і кібератак [16].

2014 р. у Литві прийнято Закон «Про Кібербезпеку», за яким кібербезпека визначається як сукупність правових, організаційних і технічних заходів для запобігання, виявлення, аналізу і реагування на кіберінциденти, а також відновлення нормального функціонування систем управління електронних мереж зв'язку, інформаційних систем або промислових процесів в разі кібератак [12].

CERT-LT є національною командою литовського Computer Emergency Response, завданням якого є забезпечення безпеки в інформаційному суспільстві шляхом запобігання, моніторингу та вирішення інцидентів інформаційної безпеки, поширення інформації про загрози інформаційної безпеки.

Метою CERT-LT є надання можливості для вирішення мережевої та інформаційної безпеки, моніторинг кіберінцидентів та їх профілактика; координація дій інтернет-провайдерів, телекомунікаційних мереж операторів і CERT груп в Литві при відповіді на мережеві та інформаційні інциденти; дослідження вразливостей мереж та інформаційних систем; поширення інформації про загрози для мережевої та інформаційної безпеки; сприяння створенню нових груп CERT [7].

Центр передового досвіду НАТО з питань енергетичної безпеки (ENSEC COE), відкрився у Вільнюсі 14 січня 2011 р. під керівництвом литовського Міністерства закордонних справ [22].

Місія Центру передового досвіду НАТО з питань енергетичної безпеки полягає в тому, щоб допомогти органам НАТО, країнам і партнерам та іншим цивільним і військовим органам шляхом надання експертних рекомендацій з усіх аспектів енергетичної безпеки. Литва та інші вісім країн вносять свій вклад в Центр, як забезпеченням кадрів, так і спільно використовуючи бюджет. В роботі Центру, в якості сприяючої країни-партнера, бере участь і Грузія.

Прагнучи стати хабом (центром) визнаних знань і досвіду в сфері енергетичної безпеки для НАТО, Центр реалізує проекти в сферах безпеки, з дотриманням трьох аспектів енергетичної безпеки у відповідності до Уельського Саміту НАТО: підвищення рівня поінформованості з питань розвитку енергетики з наслідками для безпеки, підтримка захисту критично важливої енергетичної інфраструктури та підвищення ефективності використання енергії в збройних силах. Ці компетенції забезпечуються за рахунок трьох підрозділів Центру: 1) стратегічного аналізу і досліджень, 2) освіти, підготовки і навчання, 3) доктрини та концепції розвитку [23].

Отже, країни Балтії активно намагаються реалізувати комплекс заходів для зміцнення кібербезпеки, і, звичайно, вони різняться за станом та рівнем правового, організаційного та технічного захисту інформаційного простору.

Окрім національної політики забезпечення кібербезпеки та участі в усіх програмах та проектах Альянсу, країни Балтії спільними заходами намагаються також посилити кібербезпеку регіону. Зокрема, представники трьох балтійських держав - Міністр економіки та комунікацій Естонії, Міністр оборони Латвії та Міністр національної оборони Литви 4 листопада 2015 р. підписали Меморандум про взаєморозуміння (МОВ), що стало історичним моментом для регіонального співробітництва в галузі кібербезпеки. Міністер економіки та комунікацій Естонії Крістен Міхал (Kristen Michal) сказав: «Це перший відомий тристоронній транснаціональний документ в світі з цифровим підписом» [28].

Ідея МОВ в сфері кіберспівпраці народилася ще в кінці квітня - початку травня 2007 р. на організованому НАТО семінарі з кібербезпеки, який проводили Міністерство оборони США і компанія Microsoft в штаб-квартирі останньої в Редмонді, штат Вашингтон. Учасники семінару вивчали нові можливості використання інформаційних технологій для захисту на той момент новітньої операційної системи компанії Microsoft «Windows Vista» [20, с. 19].

У 2009 р. в Ризі (Латвія) відбулася перша офіційна зустріч експертів в галузі кібербезпеки з трьох балтійських країн. Згодом вони домовилися зробити такі зустрічі регулярними і проводити їх по черзі в трьох столицях. В 2010 р. було вирішено закласти юридичну основу цих зустрічей у формі Меморандуму. Перший робочий проект меморандуму був підготовлений, обговорений і модифікований на наступних зустрічах. Цей процес тривав кілька років через кадрові зміни і переходу завдань з координування політики в галузі національної кібербезпеки до інших відомств. Наприклад, в Латвії змінилося відомство з Міністерства транспорту і комунікацій на Міністерство оборони, в той час як в Литві остання зміна відбулася в січні 2015 р., коли відповідальність за координування політики було покладено на Міністерство національної оборони відповідно до прийнятого в грудні 2014 р. Закону «Про кібербезпеку». Ця остання зміна забезпечила стабільність в плані відомчої координації в питаннях остаточного оформлення і ратифікації проекту МОВ владою кожної країни і

підготовки до офіційного підписання, яке було заплановано на весну 2015 р. Однак офіційне підписання довелося відкласти на кілька місяців, через те що додатково було необхідно скористатися найбільш сучасними технологіями електронного підпису. Отже, щоби всі три національні електронні підписи на одному і тому ж документі були визнані кожним підписантом, довелося подолати багато технічних труднощів. Зокрема, кожна з країн Балтії використовує свій власний формат цифрового підпису - Естонія використовує BDOC, Латвія і Литва EDOC ADOC - тому міністри підписали три документи в іншому форматі, одного й того ж змісту. Всі три формати діють у всьому Європейському Союзі [20, с. 20].

Меморандум про взаємодопомогу встановлює юридичну основу цього регіонального співробітництва та визначає спільні види діяльності, що включають:

• обмін знаннями та досвідом для сприяння розвитку політик та практик кібербезпеки;

• наголос на види співробітництва, які можуть знизити ризики і уразливості, пов'язані з транскордонними залежностями між незалежними інформаційними системами, мережами і критичною інфраструктурою;

• обмін інформацією про виявлені кіберінциденти, які можуть вплинути на кіберпростір інших країн-учасниць;

• обмін інформацією про раннє виявлення потенційних атак, спрямованих на інформаційні системи або мережі інших країн-учасниць;

• визначення контактних пунктів і обмін контактними даними для звичайного і екстреного зв'язку [20, с. 22].

Знадобилося кілька місяців, перш ніж вдалося домогтися того, щоб різне програмне забезпечення по роботі з електронними підписами і різні стандарти могли застосовуватися і визнаватися всіма сторонами, що надало балтійським країнам можливість познайомитися з технологіями електронного підпису своїх сусідів. Вирішення проблем, що виникали поглибило технічні знання фахівців, що може в подальшому допомогти підвищити популярність електронних підписів в балтійських країнах.

Джерела та література:

1. Впровадження європейської кібербезпеки: загальний огляд [Електронний ресурс]. – ISACA, 2015. – 27 с. – Режим доступу: https://

www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf

2. Глобальная программа кибербезопасности МСЭ 2007 г. Основа для международного сотрудничества в области кибербезопасности [Електронний ресурс]. – Режим доступу: http://gosbook.ru/node/23428

3. Глобальный индекс кибербезопасности и профили по киберблагополучию. Отчет. Апрель 2015 года. – МСЭ, 2015. – 528 с. – Режим доступу: http://www.itu.int/ru/ITU-D/Pages/Global-Cybersecurity-Index-and-Cyberwellness-Profiles-Report.aspx

4. Резолюция 130 « Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий». Полномочная конференция Международного союза электросвязи [Електронний ресурс] // Заключительные акты Полномочной конференции Международного союза электросвязи (Пусан, 2014 г.). – ITU, 2015. – С. 241-299. – Режим доступу: http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000544001PDFR.PDF

5. About CERT Estonia [Електронний ресурс]. – Режим доступу: https://www.ria.ee/en/cert-estonia.html

6. CERT.LV [Електронний ресурс]. – Режим доступу: https://www.cert.lv/lv/par-mums

7. CERT-LT [Електронний ресурс]. – Режим доступу: https://www.cert.lt/en/

8. Cyber Security Strategy 2014–2017. Ministry of Economic Affairs and Communication 2014 [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf

9. 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

10. Cyber Security Strategy.Committee Ministry of Defence Estonia Tallinn [Електронний ресурс]. – 2008. – Режим доступу: https://www.unodc.org/res/cld/lessons-learned/cyber-security-strategy_html/Cyber_Security_Strategy_Estonia.pdf

11. eGovernment in Estonia, February 2016, Edition 18.0. [Електронний ресурс]. – European Union, 2015. – 53 p. – Режим доступу: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGo

vernment%20in%20Estonia%20-%20February%202016%20-%2018_00_v4_00.pdf

12. National legislation Cybersecurity Act (2014) [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/sites/default/files/strategy/LTU_CSAct_lt.pdf

13. NATO Strategic Communications Centre of Excellence Riga, Latvia [Електронний ресурс]. – Режим доступу : http://www.stratcomcoe.org/

14. NATO Strategic Communications Centre of Excellence. Report for the period from 1 January 2015 to 31 December 2015 [Електронний ресурс]. – P. 18. – (30 P) Режим доступу: http://www.stratcomcoe.org/audited-annual-report-2015

15. NATO Strategic Communications Policy [Електронний ресурс]. – Режим доступу: http://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

16. Resolution no 796 of 29 June 2011. On the Approval of The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019 [Електронний ресурс]. – Режим доступу: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

17. Залищук С. Принять вызов /С. Залищук // Новое время. – 2017. – № 7. – С. 63.

18. Шаповал Е. Нам и не снилось /Е. Шаповал // Новое время. – 2017. – № 7. – С. 58-59.

19. Баровська А.В. Стратегічні комунікації: досвід НАТО [Електронний ресурс] /А.В. Баровська // Стратегічні пріоритети. – 2015. – № 1 (34). – С. 147-151. – Режим доступу: http://sp.niss.gov.ua/content/articles/files/24-1436781085.pdf

20. Бутримас Витаутас. Балтийское сотрудничество в области кибербезопасности [Електронний ресурс] / Бутримас Витаутас // per Concordiam. – 2016. – № 2. – Том 7. – С. 19-23. – Режим доступу: http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pC_V7N2_ru.pdf

21. В Латвии открылся новый офис Центра стратегических коммуникаций НАТО. 20 августа 2015 [Електронний ресурс]. – Режим доступу: ТАСС:http://tass.ru/mezhdunarodnaya-panorama/2198715

22. Високопоставлені представники НАТО взяли участь у церемонії відкриття Центру енергетичної безпеки у Вільнюсі, Литва. 14

січня 2011 р. [Електронний ресурс]. – Режим доступу: http://www.otan.nato.int/cps/uk/natohq/news_69826.htm?selectedLocale=uk

23. Вступне слово Н. Багдонаса. Директор Центру передового досвіду НАТО з питань енергетичної безпеки [Електронний ресурс] // Невоєнний вимір війн нового покоління. Енергетичний компонент Матеріали за підсумками міжнародної конференції. – К.: НІСД, 2016. – Режим доступу: http://niss.gov.ua http://geostrategy.org.ua http://qclub.org.ua

24. Замікула М. Країни Балтії – НАТО: боротьба з кібертероризмом [Електронний ресурс] /М. Замікула // Вісник Наукового інформаційно-аналітичного центру НАТО Прикарпатського національного університету імені Василя Стефаника. – 2009. – № 2. – С. 54-58. – Режим доступу: http://nato.pu.if.ua/journal/2009/2009-12.pdf

25. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки [Електронний ресурс] /О.Ю.Запорожець // Актуальні проблеми міжнародних відносин. Випуск 87 (Частина ІІ), 2009. – С. 36-43. – Режим доступу: http://journals.iir.kiev.ua/index.php/apmv/article/viewFile/1195/1139

26. Нигяр Джафарли. В Риге торжественно открыли Центр стратегических коммуникаций НАТО. Рига, 20 августа [Електронний ресурс]. – Режим доступу: https://mpsh.ru/print:page,1,2232-v-rige-torzhestvenno-otkryli-centr-strategicheskih-kommunikaciy-nato.html

27. Тамм Ильмар. П-к. Слияние кибер- и национальной безопасности [Електронний ресурс] /Ильмар Тамм // per Concordiam. – 2011. – № 2. – Том 2. – С. 8-9. – Режим доступу: http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pC_V2N2_ru.pdf

28. Baltic ministers digitally sign cyber security agreement. BC, Tallinn, 05.11.2015 [Електронний ресурс]. – Режим доступу: http://www.baltic-course.com/eng/Technology/?doc=11254

29. State information system [Електронний ресурс]. – Режим доступу: https://www.mkm.ee/en/objectives-activities/information-society/state-information-system

30. The Estonian Informatics Centre became the Estonian Information System's Authority. 16.06.2011 [Електронний ресурс]. – Режим доступу: https://www.ria.ee/en/the-estonian-informatics-centre-became-the-estonian-information-systems-authority.html