УДК 004.056.5(.476)(.063)

Н. Ф. Казакова, д.т.н., **О. О. Фразе-Фразенко,** к.т.н., **Є. Є. Паладій, Айвазова К. Б.**

Одеська державна академія технічного регулювання та якості, м. Одеса

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВНІ НАПРЯМКИ АДАПТАЦІЇ НОРМАТИВНОЇ БАЗИ УКРАЇНИ ДО НОРМ ЄС ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

Проведений огляд сучасного досвіду із забезпечення захисту державних інформаційних ресурсів у країнах з розвинутою інформаційною та телекомунікаційною інфраструктурами, з точки зору аналізу тенденцій у державній, бюджетній, інвестиційній, науково-технічній та кадровій політиці, а також, з вирішення комплексу проблем, пов'язаних із забезпеченням інформаційної безпеки всієї національної інформаційної інфраструктури.

***Ключові слова**: інформаційна безпека, інформаційно-вимірювальні системи, кібербезпека, системи захисту інформації*

Вступ

Сьогодні інформаційна безпека держави, як самостійний напрям сучасних технологій, без тіні перебільшення переживає своє друге народження. Особливість нинішнього етапу розвитку не тільки інформаційних, але й практично всіх технологій характеризується надзвичайно високим ступенем їх інтеграції до усіх сфер людської діяльності та зумовленою цією обставиною взаємозалежністю і потенційною вразливістю. Потоки інформації, пов'язані з виробництвом, закупівлею та продажем товарів, наданням послуг, банківськими та фінансовими операціями, нормативно-правовою та законодавчою діяльністю, постійно наростають. Глобалізація стає визначальним чинником існування та виживання сучасної цивілізації. Світ підійшов до тієї межі, коли кордони між державами перестали бути нездоланними бар'єрами не тільки для бізнесу та торгівлі, науки та освіти, відпочинку та розваг, а й для тероризму, злочинності та наркоманії [1, 2]. Наслідки від численних деструктивних впливів на світовий військово-політичний стан, економіку, суспільно-соціальні та науково-технічні відносини є підтвердженням цього. У зв'язку з цим, досвід щодо забезпечення захисту державних інформаційних ресурсів у країнах з розвинутою інформаційною та телекомунікаційною інфраструктурами, представляється досить цікавим і повчальним з точки зору аналізу тенденцій у державній, бюджетній, інвестиційній, науково-технічній та кадровій політиці, а також, що є найбільш важливим, з вирішення комплексу проблем, пов'язаних із забезпеченням інформаційної безпеки всієї національної інформаційної інфраструктури (НІІ) [3].

Аналіз останніх досліджень та публікацій

Так, у США, вже багато років діє «Національний план захисту інформаційних систем» [4]. Згідно до нього були створені Рада по безпеці національної інфраструктури (англ. : *National Infrastructure Concil*, NIAC) та спеціальні центри комп'ютерної та інформаційної безпеки: у Пентагоні – Об'єднана оперативна група з захисту комп'ютерних мереж (англ.: *Joint Task Force for Computer Network Defense,* JTF-CND), у ФБР – Національний центр захисту інфраструктури (англ.: *National Infrastructure Protection Center,* NIPC). Крім того, створені Національний та Федеральний центри реагування на комп'ютерні події та інциденти інформаційної безпеки (англ.: *National Security Incident Response Center*, NSIRC; *Federal Computer Incident Response Center,* FedCIRC), які за допомогою спеціальної федеральної мережі виявлення вторгнення (англ.: *Federal Intrusion Detection Network*, FIDNet) сповіщають урядовим, промисловим, комерційним та громадським організаціям про загрозу інформаційного нападу на країну [5].

Згідно [6, 7], більша частина витрат з державного бюджету США, які виділяються на урядові програми в області інформаційних технологій (IT) невійськового призначення йде на розвиток ресурсів Інтернету. Результати проведеного дослідження, які дають уявлення про розподіл витрат, наведені в [3, 8]. Згідно з цими джерелами, найбільш повно в урядовому домені представлені такі розділи, як економіка, суспільна безпека, ліквідація аварій та катастроф, управління ресурсами, оплата рахунків, звернення та скарги, кадрові вакансії, фінанси, закупівлі, подорожі, постачання, адміністрування. У рамках концепції «електронного уряду» (англ.: *e-Government*, eGov) [3, 9], передбачається перевести в режим online процедури, що пов'язані з проходженням паперових документів та уніфікувати форми електронних документів. Це, поряд з іншими програмами в цій області, повинно дати більшу еко-

номію бюджетних коштів з одночасним забезпеченням встановленого рівня інформаційної безпеки.

Основними стратегічними напрямами реалізації концепції eGov є напрями, які стосуються відносин уряд-громадяни, уряд-бізнес, уряд-уряд, відносини усередині установи – у рамках довіреного державного сектору. Серед програм, на яких базується eGov та функціонує FIDNet, як найбільш значимі, слід виділити «ініціативу електронної автентичності», яка повинна забезпечити необхідний рівень ідентифікації користувача, доступності та цілісності інформації, а також «проект архітектури електронного уряду», спрямований на створення міжвідомчої корпоративної інформаційної інфраструктури на основі Інтернет-технологій та сучасних стандартів представлення та захисту інформації. Структуру довіреного державного сектору мережі Інтернет для США, який функціонує на базі FIDNet, представлено у доступних першоджерелах, наприклад, у [10].

Постановка завдання

В контексті окреслених вище питань, слід зазначити що інформаційно-вимірювальні системи, як сукупність засобів вимірювальної техніки, засобів контролю, діагностування та інших технічних засобів, об'єднаних для створення сигналів вимірювальної та інших видів інформації [11] з метою надання її споживачеві (в тому числі в АСК) у потрібному вигляді є складовою великої кількості автоматизованих систем керування, в тому числі й критичного призначення. Саме тому, спираючись на вищезазначені тенденції розвитку інформаційної сфери, можна зробити висновок про необхідність приділення особливої уваги питанням стандартизації захисту інформації в інформаційно-вимірювальних системах на державному рівні. Тому, дослідження, яке присвячене огляду сучасного стану та перспективних напрямків адаптації до вимог європейського законодавства законодавчої та нормативної бази із захисту інформаційно-вимірювальних систем є актуальним.

Питання забезпечення формування і реалізації державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем криптографічного та технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України; участь у формуванні і реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування, розробленні та впровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування покладені в Україні на Державну службу спеціального зв'язку та захисту інформації.

Беручи до уваги тенденції імплементації державних стандартів до норм європейського законодавства слід зазначити, що, імплементація європейського законодавства щодо перспектив розвитку служб центрального та територіальних органів виконавчої влади, які забезпечують формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України (далі ДССЗЗІ), у своїй основі може орієнтуватися на достатньо розвинений методологічний апарат європейських агенцій, зокрема ENISA.

В рамках Європейського Союзу (ЄС) місія ENISA має важливе значення для забезпечення у всіх галузях високого та ефективного рівня мережевої та інформаційної безпеки. Її висока консолідація з державними органами держав-членів ЄС, дозволяє розвивати культуру мережевої безпеки та забезпечує інформаційну безпеку в інтересах громадян, споживачів, бізнесу та громадських організацій. В ЄС ENISA виступає в якості органу експертної оцінки специфічних технічних та наукових завдань в області інформаційної безпеки. ENISA надає практичну допомогу ЄС щодо технічної підготовчої роботи з оновлення та розробки законодавчої бази в галузі мережевої та інформаційної безпеки. ENISA створена, як результат прийняття Регламенту ЄС № 460/2004 Європейського парламенту та Ради ЄС 10 березня 2004 року. З цього моменту вона зарекомендувала себе, як найбільш компетентна організація з регулювання питань організації систем захисту інформації (СЗІ) у ЄС.

Зважаючи на достатньо вагомі рекомендації ENISA щодо забезпечення інформаційної безпеки у ЄС, встановлено, що на сучасному етапі розвитку інформаційних технологій в Україні саме нормативні документи зазначеної агенції є перспективними для розвитку вітчизняних систем захисту інформації. Аналогічний результат отримано у результаті проведення аналітичного огляду наукових публікацій, матеріалів, розміщених у мережі Інтернет, а також доступних баз патентів. Орієнтація на ENISA з метою реалізації перспектив імплементації в Україні законодавства ЄС в галузі систем захисту інформації, у достатньому ступені відповідає положенням Указу Президента України від 26.05.2015 року № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки Украї-

ни» [12] та Указу Президента України від 15.03.2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [13].

Так, наприклад:

− відповідно до п. 4.6 Указу [12] задекларована широкомасштабна адаптація законодавства України до норм і правил ЄС, забезпечення з боку України поступової конвергенції у сфері зовнішньої і оборонної політики, розвиток взаємодії у рамках Спільної безпекової і оборонної політики ЄС для посилення спроможностей сектору безпеки і оборони, а також підтримання міжнародної безпеки і стабільності;

− відповідно до п. 4.12 Указу [12] щодо забезпечення інформаційної безпеки, одним із пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів є реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав − членів НАТО та ЄС;

− відповідно до п. 4.1 Указу [13], «Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у: виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами ЄС та НАТО; створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО; …».

Висновки

Технології організації функціонування та інформаційної взаємодії існуючих в Україні інформаційних структур (ІС), мають ряд слабких сторін, усунення яких може бути розпочато у рамках адаптації до норм ЄС, а саме: необхідність автоматизованого вибору й реалізації методів і засобів аналізу й обробки даних в умовах відомих джерел первинної інформації; необхідність орієнтації ІС на різні категорії користувачів; відсутність єдиного регламенту інформаційної взаємодії й обміну даними; підтримка прийняття рішень на основі ретроспективної інформації та звітних матеріалів; технологічна та організаційна різнорідність функціональних і інформаційних компонентів ІС; децентралізована архітектура систем захисту інформації в ІС, які входять у сферу впливу держави, та ін.

Передбачається, що одним із шляхів реалізації Стратегій [12, 13] може стати впровадження документів в межах співпраці з ENISA.

Цілком логічно, що співробітництво з ENISA на державному рівні апріорі повинно спиратись на залучення широкого кола освітніх та наукових установ до підготовки та перепідготовки кваліфікованих кадрів в галузі інформаційної безпеки, світова потреба яких у зазначеній області складає близько 1 млн. осіб, що також підтверджується позитивною динамікою в межах посилення співпраці ДССЗЗІ із європейськими інституціями. А саме, за даними [14] з метою наближення законодавства України до законодавства ЄС у 2015 році ДССЗЗІ реалізовано низку заходів в рамках технічної допомоги ЄС. Зокрема, проведено два заходи у рамках проекту TAIEX на теми: «Реалізація європейської політики у сфері аудиту інформаційної безпеки (кібербезпеки)» та «Наближення політики технічного регулювання України до законодавства ЄС стосовно доступу радіообладнання і телекомунікаційного термінального обладнання на національний ринок». Які пройшли із залученням широкого кола представників органів державної влади України, науково-дослідних інститутів і телекомунікаційних компаній та експертів із Естонії, Італії, Литви, Португалії, Фінляндії, Чехії.

Список використаних джерел

1. Мелин А. Использование киберпространства террористическими и экстремистскими организациями [Текст] / А. Мелин. С. Маринин // Зарубежное военное обозрение, 2012. – № 10. – С. 3 – 8.

2. Коробов И. Использование сети Интернет террористическими и экстремистскими организациями [Текст] / И. Коробов // Зарубежное военное обозрение, 2012. – № 6(783). – С. 23 – 26.

3. Леваков А. Анатомия информационной безопасности США [Текст] / А. Леваков / Jet Info, 2002. – № 6(109). – 40 с.

4. Леваков А. А. В США принят план защиты информационных систем [Електронний ресурс] / А. А. Леваков // Портал : Jet Info. – Режим доступу \www/ URL: http://www.jetinfo.ru/2000/8/4/article4.8.2000.html. – Заголовок з екрану, доступ вільний, 08.09.2014.

5. Горбачев Ю. Обеспечение безопасности критически важной информации о состоянии вооружённых сил США [Текст] / Ю. Горбачев, О. Янов // Зарубежное военное обозрение, 2012. – № 10. – С. 21 – 31.

6. Budget of the US Government, FY 2002. Office of Management and Budget.

7. Тканова М. Проект военного бюджета США [Текст] / М. Тканова // Зарубежное военное обозрение, 2012. – № 10. – С. 15 – 20.

8. Новые приоритеты в информационной безопасности США [Текст]. – Jet Info, 2001. – № 10: Тематический выпуск. – 42 с.

9. E-Government: To Connect, Protect, and Serve Us Hart-Teeter. 1724 Connecticut Avenue, NW Washington, D.C. 20009. Council for Excellence in Government – CEG. P. 4 – 5.

10. В США готовятся к защите информационных систем [Електронний ресурс] / Портал : Agentura.ru. – Режим доступу \www/ URL: http://www.agentura.ru/equipment/psih/info/zashit/. – Заголовок з екрану, доступ вільний, 08.09.2014.

11. ДСТУ 2681-94 Державна система забезпечення єдності вимірювань. Метрологія. Терміни та визначення.

12. Стратегія національної безпеки України : Указ Президента України від 26 травня 2015 року № 287/2015 [Електронний ресурс] / Портал: rada.gov.ua. – Режим доступу \www/ URL: http://zakon5.rada.gov.ua/laws/show/287/2015. – Заголовок з екрану, доступ вільний, 10.10.2016.

13. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс] / Портал: rada.gov.ua. – Режим доступу \www/ URL: http://zakon5.rada.gov.ua/laws/show/96/2016. – Заголовок з екрану, доступ вільний, 05.10.2016.

14. Європейська інтеграція [Електронний ресурс] / Портал : dsszzi.gov.ua. – Режим доступу \www/ URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=125660&cat_id=97065&mustWords=ENISA&searchPublishing=1. – Заголовок з екрану, доступ вільний, 10.10.2016.

Поступила в редакцию 22.11.2016

Рецензент: д.т.н., проф. Братченко Г. Д., Одеська державна академія технічного регулювання та якості, м. Одеса.

Н. Ф. Казакова, д.т.н., **А. А. Фразе-Фразенко,** к.т.н., **Е. Е. Паладий, Айвазова К. Б.**

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ АДАПТАЦИИ НОРМАТИВНОЙ БАЗЫ УКРАИНЫ К НОРМАМ ЕС ПО ЗАЩИТЕ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМАХ

Проведен обзор современного опыта по обеспечению защиты государственных информационных ресурсов в странах с развитой информационной и телекоммуникационной инфраструктурами, с точки зрения анализа тенденций в государственной, бюджетной, инвестиционной, научно-технической и кадровой политике, а также, по решению комплекса проблем, связанных с обеспечением информационной безопасности национальной информационной инфраструктуры.

***Ключевые слова**: информационная безопасность, информационно-измерительные системы, кибербезопасность, системы защиты информации.*

N. F. Kazakova, DSc, **O. O. Fraze-Frazenko,** PhD, **E. E. Paladiy, K. B. Aivazova**

PRESENT STATE AND PERSPECTIVE ALIGNING THE REGULATORY FRAMEWORK OF UKRAINE TO EU NORMS ON INFORMATION SECURITY IN INFORMATION-MEASURING SYSTEMS

The current experience to ensure of government information resources in the advanced information and telecommunication infrastructures, in terms of the analysis of trends in the state, budget, investment, scientific, technical and human resources policy, as well as to address the complex issues related to information security throughout the national information infrastructure a review.

***Keywords**: information security, information-measuring systems, cyber security, information protection system.*