Запорожець О.Ю.*

ПОЛІТИКА ЄВРОПЕЙСЬКОГО СОЮЗУ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

The article focuses on the European Union's approach to the information security as well as to the fight against cybercrime. Besides conceptual aspects of EU policy the practice of information security policy implementation on national level is studied. Two leading countries in information security area Finland and Estonia are chosen as examples.

Домінантною рисою сучасних міжнародних відносин є стрімкий розвиток інформаційного суспільства, основу якого складають інформаційно-комунікаційні технології (ІКТ). Для інформаційного суспільства характерне перманентне вдосконалення інформаційних технологій й швидкі темпи їхнього впровадження у всі сфери суспільного життя. Результатом є віртуалізація значної частини суспільних відносин (розвиток державних он-лайн послуг, е-комерції, дистанційного навчання та ін.) і посилення залежності країн від електронних мереж та інформаційних систем.

Важливими тенденціями сучасного етапу розвитку людства є також інтенсифікація транскордонних інформаційних потоків, поширення різноманітних способів і засобів інформаційного обміну, які практично не контролюються державою. За цих умов набувають поширення нові – інформаційні – загрози та виклики, що вимагають від держав негайного реагування й застосування нестандартних заходів і рішень. В зв'язку з цим пріоритетним питанням «порядку денного» на міжнародному, регіональному та національному рівнях стає інформаційна безпека.

Активну політику в сфері інформаційної безпеки проводить Європейський Союз. Сьогодні Європейський Союз об'єднує високо розвинуті країни, які здійснюють неабиякий вплив на міжнародні відносини, встановлюючи норми і стандарти поведінки держав в політичній, економічній, соціальній, інформаційній та інших сферах. За цих умов актуальним є комплексне дослідження європейського підходу до інформаційної безпеки, особливо зважаючи на євроінтеграційні прагнення України.

В сучасній літературі досліджено окремі аспекти інформаційної безпеки. Залежно від висвітлюваних питань, публікації на тему європейської інформаційної безпеки можна розділити принаймні на такі групи: 1) механізми та правове забезпечення захисту інформації в європейських країнах; 2) безпека е-врядування та захист персональних даних в країнах ЄС; 3) загальна концепція політики інформаційної безпеки ЄС, ОБСЄ та НАТО; 4) сучасні інформаційні загрози і виклики, для європейських країн зокрема; 5) інформаційна безпека України в контексті європейської інтеграції тощо.

Метою даної роботи є всебічне висвітлення пріоритетних напрямів діяльності ЄС в сфері інформаційної безпеки та механізмів їхньої реалізації на національному рівні (на прикладі Фінляндії та Естонії).

В 2001 році Європейською Комісією було представлено перший документ під назвою *«Мережева та інформаційна безпека: європейський політичний підхід»* (Network and In-

* асистент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка, кандидат політичних наук

formation Security: Proposal for A European Policy Approach), в якому окреслено європейський підхід до проблеми інформаційної безпеки. У документі використовується термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [1].

Дії, що порушують безпеку інформаційних мереж і систем, згруповані таким чином: перехоплення електронної комунікації, копіювання або модифікація даних; неавторизований доступ до комп'ютера або комп'ютерних мереж; деструктивні атаки на мережі, зокрема атаки на доменні імена, перевантаження мережі штучними повідомленнями, атаки, спрямовані на порушення маршрутизації; шкідливе програмне забезпечення; підробка веб-сайтів; безпекові інциденти як наслідок непередбачених і ненавмисних подій, таких як природні катаклізми, збої у роботі апаратних засобів та програмного забезпечення, людські помилки.

В документі визначено такі основні напрями європейської політики інформаційної безпеки:

1. *Підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами.*

В рамках цього напряму пріоритетними заходами є проведення інформаційно-освітніх кампаній для громадськості, просування кращого досвіду у сфері безпеки, а також розвиток навчальних курсів, присвячених питанням безпеки.

2. Створення європейської системи попередження та інформування про нові загрози.

Основне завдання країн ЄС – створити систему попередження для користувачів, яка б не лише інформувала про небезпеку, але й давала поради щодо протидії атакам, а також створити конфіденційний механізм сповіщення про атаки для бізнесових структур. Для цього передбачено такі заходи, як перегляд країнами-членами технічного забезпечення та компетенції національних комп'ютерних груп швидкого реагування (CERT) та розвиток співпраці комп'ютерних груп швидкого реагування Євросоюзу з подібними структурами інших країн.

3. *Забезпечення технологічної підтримки.*

Пріоритетне значення надається розвитку досліджень з проблеми мережевої та інформаційної безпеки. Для цього пропонується включати питання безпеки у Рамкові дослідницькі програми ЄС, а країнам-членам рекомендується активно просувати використання засобів змінного стійкого шифрування.

4. *Підтримка ринково орієнтованої стандартизації та сертифікації.*

Основною проблемою ЄС є існування великої кількості конкуруючих стандартів та специфікацій в сфері інформаційної безпеки, що призводить до фрагментації ринку та несумісних рішень. Для вирішення проблеми передбачається перегляд існуючих стандартів безпеки; розвиток сумісних і безпечних продуктів і послуг; заохочення використання процедур сертифікації та акредитації по загальноприйнятим європейським та міжнародним стандартам тощо.

5. *Правове забезпечення.*

Пріоритетними напрямами політики ЄС в сфері правового регулювання інформаційної безпеки є захист персональних даних, телекомунікаційні послуги та кіберзлочинність. За цим напрямом передбачено такі заходи, як забезпечення спільного розуміння правових наслідків безпеки в електронних комунікаціях; створення країнами-членами сприятливих умов для вільного обігу продуктів і послуг шифрування через гармонізацію адміністративних експортних процедур та послаблення експортного контролю; розробка

Комісією правових заходів для зближення національних законодавств щодо атак на комп'ютерні системи.

6. *Зміцнення безпеки на державному рівні.*

Проблема безпеки має важливе значення для подальшого розвитку е-врядування. Основним завданням державних органів влади є сприяння розвитку культури безпеки. За цим напрямом передбачається впровадження ефективних і сумісних засобів інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних он-лайн послуг тощо.

7. *Розвиток міжнародного співробітництва з питань інформаційної безпеки.*

Основне завдання ЄС – зміцнення діалогу Європейської Комісії з міжнародними організаціями та партнерами щодо проблеми мережевої безпеки та, зокрема, щодо зростаючої залежності від електронних мереж.

10 березня 2004 року було створено *Європейську агенцію з питань мережевої та інформаційної безпеки* (European Network and Information Security Agency - ENISA), діяльність якої спрямована на зміцнення можливостей європейської спільноти, країн-членів, а також ділових кіл в сфері попередження і реагування на проблеми, пов'язані з інформаційною безпекою.

Основними напрямами діяльності Агенції є: надання консультацій та допомоги Комісії і країнам-членам в сфері інформаційної безпеки; збір та аналіз даних щодо безпекових інцидентів в Європі та ризиків, що виникають; розробка методів оцінки та управління ризиками для підвищення здатності ЄС реагувати на загрози інформаційній безпеці; підвищення обізнаності та розвиток співробітництва між різними акторами в сфері інформаційної безпеки, зокрема шляхом стимулювання взаємодії між державним і приватним секторами. Агенція також допомагає Європейській Комісії у попередній технічній роботі з метою оновлення і вдосконалення європейського законодавства в сфері мережевої та інформаційної безпеки [2].

У своїй діяльності Агенція спирається на щорічні робочі плани/програми, які містять перелік основних пріоритетів і цілей та запланованих заходів для виконання поставлених завдань. Так, у робочій програмі Агенції на 2010 рік визначено такі стратегічні пріоритети, як підвищення здатності європейських електронних мереж протистояти зовнішнім впливам; розвиток співробітництва між країнами-членами в сфері інформаційної безпеки; ідентифікація нових ризиків в сфері інформаційної безпеки і формування взаємної довіри між зацікавленими особами у реагуванні на нові ризики.

В рамках ЄС значна увага приділяється проблемі кібербезпеки як складової інформаційної безпеки. З 1999 року ЄС реалізує програми «Безпечніший Інтернет» (Safer Internet). Тривалість кожної програми – 4-5 років. В рамках програми «Безпечніший Інтернет» на 2009-2013 роки передбачено низку заходів, спрямованих не лише на боротьбу зі шкідливим контентом, але й з небезпечною поведінкою в мережі [3]. Основними цілями програми є підвищення обізнаності громадськості, забезпечення громадськості мережею контактних пунктів для повідомлення про незаконні та шкідливі контент і поведінку; сприяння саморегулюючим ініціативам у цій сфері та залучення дітей до створення безпечнішого он-лайн середовища; створення бази знань щодо нових тенденцій у використанні он-лайн технологій та їхніх наслідків для життя дітей.

Так, в рамках програми фінансуються Інтернет-центри, які створюються на національному рівні і координуються на європейському рівні. Основна мета діяльності центрів – підвищення обізнаності дітей, батьків, вчителів про он-лайн ризики, а також надання порад молоді щодо безпечного користування мережею через телефони довіри та контактні пункти. Загалом, на сьогодні в рамках програми «Безпечнійши Інтернет» фінансується понад 30 проектів.

У травні 2007 році Європейською Комісією представлено документ *«На шляху до загальної політики в сфері боротьби з кіберзлочинністю»*, в якому «кіберзлочинність» визначається як кримінальні дії, скоєні з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем. Це поняття включає три категорії злочинів: 1) традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); 2) публікація протизаконного контенту в електронних медіа (дитяча порнографія, матеріали із закликами до расової ненависті і т.п.); 3) специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо) [4].

Політика Європейської Комісії в сфері боротьби з кіберзлочинністю реалізується за чотирма основними напрямами. По-перше, це законотворчий процес. Найбільш важливим законодавчим рішенням є Рамкове рішення Ради Міністрів ЄС щодо атак на інформаційні системи від 17 січня 2005 року. Рамкове рішення покликане забезпечити мінімальний рівень зближення кримінального права для найбільш поширених форм кримінальної діяльності відносно інформаційних систем, таких як незаконний доступ, незаконне втручання у систему та дані. По-друге, Європейська Комісія заохочує транскордонне співробітництво правоохоронних органів країн-членів ЄС шляхом організації конференцій, створення цілодобових контактних пунктів у країнах-членах ЄС, розвитку платформи для навчання експертів у сфері боротьби з кіберзлочинністю. По-третє, Європейська Комісія розвиває співробітництво між державним і приватним секторами у боротьбі з кіберзлочинністю, зокрема, співпрацю між правоохоронними органами та приватними компаніями. По-четверте, Європейська Комісія заохочує підписання країнами-членами та іншими країнами Конвенції про кіберзлочинність, розробленої Радою Європи, та бере участь у міжнародних робочих групах.

В березні 2009 року опубліковано Повідомлення Європейської Комісії під назвою *«Захист Європи від широкомасштабних кібер-атак та руйнувань: посилення рівня підготовленості, безпеки та стійкості»*, в якому визначено основні виклики/проблеми, які потребують негайного реагування ЄС, а також окреслено основні заходи, необхідні для посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам [5].

Згідно з документом, основними викликами безпеці інформаційних інфраструктур ЄС є некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів; відсутність на європейському рівні партнерства між державним та приватним секторами; обмежені можливості ЄС щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем; відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури

Для ефективного реагування ЄС на існуючі виклики кібербезпеці необхідна реалізація низки заходів:

1. Забезпечення належного рівня підготовки на всіх рівнях, що передбачає визначення країнами-членами базових можливостей для національних Комп'ютерних команд швидкого реагування та систем реагування на безпекові інциденти; посилення співпраці між державним і приватним секторами; створення європейського форуму для обміну інформацією між країнами-членами;

2. Створення європейської системи раннього сповіщення про кіберзагрози;

3. Зміцнення захисних механізмів для критичної інформаційної інфраструктури ЄС, що передбачає розробку національних планів реагування на надзвичайні події та органі-

зацію тренінгів для широкомасштабного реагування на безпекові інциденти; проведення панєвропейських навчань з проблеми безпекових інцидентів у мережі Інтернет; зміцнення співпраці між національними комп'ютерними групами швидкого реагування;

4. Вироблення європейських керівних принципів щодо забезпечення стійкості і стабільності мережі Інтернет та їхнє просування на міжнародній арені;

5. Визначення критеріїв ідентифікації європейської критичної інфраструктури для сектору інформаційно-комунікаційних технологій.

Політичні пріоритети в сфері інформаційної безпеки, визначені керівними органами Європейського Союзу, втілюються у життя на національному рівні як органами державної влади, так і неурядовими організаціями.

Однією з країн-лідерів ЄС за показниками розвитку інформаційного суспільства є **Фінляндія**. В рейтингу країн ЄС Фінляндія займає перше місце за рівнем цифрової грамотності (понад 50% населення), друге місце – за показником поширення мережі широкосмужного зв'язку (34% населення) [6].

Основними державними установами, відповідальними за розробку та реалізацію політики інформаційної безпеки, є Міністерство транспорту та комунікацій та Омбудсмен з питань захисту даних (Data Protection Ombudsman) тощо.

Повноваженнями *Міністерства транспорту та комунікацій* є розробка законодавства щодо комунікаційних мереж, безпеки даних, забезпечення доступу до комунікаційних послуг, а також розробка і реалізація національної політики в сфері інформаційної безпеки.

В грудні 2008 року урядом Фінляндії прийнято Національну стратегію інформаційної безпеки на 2009-2015 рр. [7]. В Стратегії визначено п'ять пріоритетних цілей державної політики в сфері інформаційної безпеки: розвиток співробітництва з питань інформаційної безпеки на національному та міжнародному рівнях; підтримання національної конкурентоспроможності та створення сприятливих умов для національних операторів інформаційно-комунікаційних технологій; вдосконалення системи управління ризиками в сфері інформаційної безпеки; забезпечення захисту основоположних прав громадян та інтелектуального капіталу країни; підвищення громадської обізнаності в сфері інформаційної безпеки.

Структурним підрозділом Міністерства транспорту та комунікацій є Управління Фінляндії з регулювання комунікацій (Finnish Communications Regulatory Authority – FICORA), яке уповноважене здійснювати контроль та державне регулювання у сфері інформаційно-комунікаційних технологій [7]. До повноважень FICORA відноситься контроль функціональності електронних комунікаційних мереж, інформування про можливі загрози інформаційній безпеці, підвищення обізнаності громадян з питань інформаційної безпеки, планування і управління використанням радіочастот, мережевими адресами, а також контроль змісту програм і реклами на телебаченні та радіо.

В структурі FICORA функціонує CERT-FI (Computer Emergency Response Team of Finland) – фінська комп'ютерна група швидкого реагування, основним завданням якої є попередження, виявлення та реагування на інциденти у сфері інформаційної безпеки, а також поширення інформації про загрози інформаційній безпеці. До компетенції CERT-FI відноситься: проведення моніторингу інцидентів на національному рівні; підтримання обізнаності громадськості про загрози інформаційній безпеці; вироблення рекомендацій для зміцнення інформаційної безпеки; поширення інформації про способи попередження інцидентів, пов'язаних з інформаційною безпекою; надання допомоги у вирішенні проблем у сфері інформаційної безпеки; співробітництво з постачальниками обладнання та програмного забезпечення, з правоохоронними органами; проведення моніторингу і аналізу загроз інформаційній безпеці на міжнародному рівні тощо [8].

Омбудсмен з питань захисту даних (Data Protection Ombudsman) - незалежний орган, уповноважений забезпечити захист права громадян на недоторканість приватного життя шляхом здійснення контролю за обробкою персональних даних та надання консультацій з цих питань. Омбудсмен спільно з FICORA видає спеціалізований журнал «Tietosuoja», що містить інформацію про норми і практику в сфері захисту даних, про безпеку даних в електронних системах комунікації, а також вимоги ЄС щодо рівня захисту даних в країнах-членах [6].

Серед неурядових організацій, які займаються питаннями інформаційної безпеки, провідна роль належить Фінській федерації комунікацій та телеінформатики (Finnish Federation for Communications and Teleinformatics – FiCom) та Фінській асоціації з питань інформаційної безпеки (Finnish Information Security Association) [6].

Ф*інська федерація комунікацій та телеінформатики* об'єднує компанії, що працюють у сфері інформаційно-комунікаційних технологій. Основна мета діяльності федерації – розвиток бізнес-можливостей своїх членів та підвищення їхньої конкурентоспроможності. Діяльність FiCom включає планування і координацію заходів щодо розвитку інформаційно-комунікаційних технологій, здійснення моніторингу ситуації в ІКТ-секторі, здійснення впливу в сфері регулювання ринку інформаційно-комунікаційних технологій тощо.

Фінська асоціація з питань інформаційної безпеки є найбільшою неприбутковою асоціацією Фінляндії в сфері інформаційної безпеки, яка функціонує з 1997 року й об'єднує понад 90 членів. Метою діяльності асоціації є розвиток професіоналізму й обізнаності в сфері інформаційної безпеки. Діяльність асоціації включає організацію дискусій, конференцій, участь у різних програмах з інформаційної безпеки.

В країні реалізується низка програм в сфері інформаційної безпеки, що фінансуються урядом Фінляндії. Такими програмами є Фінський проект з Інтернет-обізнаності та безпеки (The Finnish Internet Awareness and Safety project), Проект TrustInet та Інтернет-автобус (Internet Bus) [6].

Фінський проект з Інтернет-обізнаності та безпеки, розрахований на період 2008-2010 роки, є спільним проектом трьох організацій: «Save the Children Finland», Ліга захисту дітей імені Маннергейма (The Mannerheim League for Child Welfare) та FICORA. Метою проекту є просування безпечного користування мережею Інтернет та боротьба з незаконним контентом. В рамках проекту реалізуються такі заходи, як організація Дня безпечного Інтернету, створення навчальних програм з питань безпеки Інтернет для провайдерів веб-контенту, встановлення «телефону довіри» для користувачів Інтернет для повідомлення про незаконний контент та інші проблеми.

Суть проекту *TrustInet* полягає у дослідженні проблеми довіри у відносинах між провайдерами послуг та споживачами в мережі Інтернет. Проект фінансується Державним агентством фінансування технологій та інновацій (Finnish Funding Agency for Technology and Innovation - Tekes).

З червня 2001 року реалізується проект *«Інтернет-автобус*», що має за мету навчити людей працювати з комп'ютерами та користуватися мережею Інтернет. У фінському місті Тампере їздить яскраво розмальований автобус «Netti-Nysse», обладнаний комп'ютерами, в якому проводяться навчальні курси з комп'ютерної грамотності.

Серед країн Центрально-Східної Європи, які отримали членство в ЄС, провідне місце у розробці і впровадженні політики інформаційної безпеки посідає Естонія. Розробка і впровадження політики інформаційної безпеки належить до компетенції Міністерства економіки та комунікацій, а точніше таких його структурних підрозділів, як Департамент державної інформаційної системи та Естонський центр інформатики [6].

Департамент державної інформаційної системи уповноважений координувати політичну діяльність в сфері інформаційних технологій та розробляти плани в сфері державних адміністративних інформаційних систем, а саме: державні ІТ-бюджети, законодавство в сфері інформаційних технологій, координація ІТ-проектів, ІТ-аудити, стандартизація, міжнародне співробітництво в сфері державних інформаційних систем.

Естонський центр інформатики є виконавчим органом у загальній системі координації державної інформаційної політики та розвитку державного сектору інформаційних технологій. Основне завдання Центру – координувати розробку і управління державною інформаційною системою. До компетенції Центру відноситься управління проектами, включаючи підготовку ІТ-проектів для державних інституцій; проведення моніторингу ситуації з інформаційними технологіями; створення державних реєстрів; розвиток комп'ютерних мереж; вироблення правових засад у сфері інформаційних технологій; здійснення державних закупівель інформаційних технологій тощо.

Міністерством економіки та комунікацій Естонії розроблено національну політику інформаційної безпеки. Основна мета політики Естонії в сфері інформаційної безпеки – створення безпечного і відкритого для міжнародної співпраці інформаційного суспільства. Більш конкретними цілями політики інформаційної безпеки є усунення неприйнятних ризиків, захист основних прав людини, забезпечення обізнаності та тренінгів в сфері інформаційної безпеки, участь у міжнародних ініціативах з е-безпеки, а також підвищення конкурентоспроможності економіки.

8 травня 2008 року урядом Естонії затверджено *Стратегію кібербезпеки Естонії* на 2008-2013 роки [9]. 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.

Діяльність щодо захисту критичної інформаційної інфраструктури включає: визначення послуг, необхідних для функціонування критичної інформаційної інфраструктури; розробку загальної методології оцінки вразливості інформаційних систем критичної інфраструктури; збір та обробку інформації щодо поточної ситуації у кіберпросторі для планування превентивних заходів та контрзаходів у сфері національної кібербезпеки тощо.

Розробка та впровадження системи заходів безпеки передбачає, зокрема, визначення мінімального рівня функціональності інформаційної інфраструктури та забезпечення цього рівня функціонування у кризовій ситуації; визначення заходів протидії у надзвичайній ситуації, якщо на об'єкти критичної інфраструктури здійснено атаку; розробка методів тестування для засобів безпеки; вдосконалення систем ідентифікації та моніторингу електромагнітного впливу на критичну інфраструктуру; зміцнення інфраструктури Інтернет; підвищення безпеки систем контролю тощо.

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.

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.

Діяльність щодо правового регулювання сфери кібербезпеки включає розробку правових визначень кібербезпеки та кіберзлочину; впровадження законодавства щодо питань кібербезпеки, включаючи запровадження обов'язкових заходів та стандартів безпеки і встановлення мінімальних вимог до безпеки інформаційних систем тощо.

Діяльність щодо зміцнення міжнародної співпраці з питань кібербезпеки передбачає винесення проблем кібербезпеки на міжнародний «порядок денний»; сприяння ратифікації країнами Конвенції Ради Європи про кібезлочинність; обговорення проблем кібербезпеки на конференціях, семінарах та форумах; просування кращої практики в сфері кібербезпеки на міжнародному рівні тощо.

Важливу роль у вирішенні проблем інформаційної безпеки в Естонії відіграє *Естонська інспекція захисту даних*. Це установа державного нагляду, основними напрямами діяльності якої є надання правової допомоги і здійснення контролю (надання порад, роз'яснення, розгляд скарг, здійснення перевірок, участь у діяльності європейських організацій з питань захисту даних); створення баз даних державного сектору; реєстрація обробки конфіденційних персональних даних; авторизація обробки даних; здійснення адміністративного примусу та виконання наказів щодо правової відповідальності тощо [10].

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 Естонії також функціонує декілька неурядових організацій, які роблять свій внесок у зміцнення інформаційної безпеки держави. Серед них - Фонд Look@World та Центр сертифікації.

В 2001 році десять провідних компаній Естонії створили *Фонд Look@World* з метою підвищення кількості Інтернет-користувачів в країні. Фондом реалізовано такі проекти, як тренінги з користування комп'ютерами та мережею Інтернет для 100 тисяч громадян, створення середовища eSchool, відкриття 500 пунктів доступу до мережі Інтернет.

23 травня 2006 року основні учасники Фонду Look@World та Міністерство економіки і комунікацій Естонії підписали договір про співпрацю щодо започаткування загальнонаціональної ініціативи під назвою «Комп'ютерний захист 2009» (Computer Protection 2009). Мета проекту – до 2009 року перетворити Естонію на країну з найбільш безпечним інформаційним суспільством у світі [11].

За договором, сторони зобов'язуються забезпечити стійкий розвиток е-послуг та ІТ-рішень, що надаються державою та приватним сектором; дати можливість користувачам е-послуг активно брати участь у захисті інформаційного суспільства, зберігаючи при цьому стабільне середовище та довіру до цих послуг; сприяти заходам із підвищення обіз-

наності та вдосконалення навичок, пов'язаних із ІТ-безпекою; створити умови для підвищення простоти, доступності та зручності у користуванні апаратних засобів та програмного забезпечення. Сторони домовилися також об'єднати зусилля для забезпечення розробки і впровадження додатків на базі ідентифікаційної картки (ID card) та сучасної криптографічної системи з відкритим ключем.

Діяльність Фонду Look@World в рамках ініціативи «Computer Protection 2009» полягає у наступному: просування і пріоритетний розвиток ідентифікаційних карток; інтеграція ідентифікаційної картки та інших механізмів ідентифікації на базі технології PKI (Public Key Infrastructure) у свої послуги та забезпечення максимального використання цифрового підпису у бізнес-процесах; інвестування в інфраструктуру та подібні послуги; проведення тренінгів та надання інформації естонським громадянам щодо користування ідентифікаційною карткою в електронних системах; надання консультацій підприємствам та установам щодо розвитку послуг на базі ідентифікаційних карток; створення і підтримка порталу, присвяченого безпеці інформаційних технологій; розробка показників Інтернет-безпеки тощо.

З метою інформування громадськості про ідентифікаційну картку як найбільш простий та безпечний механізм самозахисту під час використання е-послуг створено сайт http://koolitus.id.ee, на якому пояснюється, чому необхідна ідентифікаційна картка, як її отримати, як нею користуватися, як зробити електронний підпис тощо. Інформація доступна естонською та російською мовою.

В лютому 2001 року двома провідними банками Естонії Hansapank і SEB спільно з двома телекомунікаційними компаніями Elion і EMT створено Центр сертифікації. Це єдина установа в Естонії, яка видає сертифікати на аутентифікацію та електронний підпис для ідентифікаційних карток. Центр не лише видає сертифікати на ідентифікаційні картки, але й надає послуги, пов'язані із юридичною дієвістю сертифікатів та використанням електронних підписів. Послугами Центру користуються естонські банки, судові органи і нотаріуси, правоохоронні органи, Республіки Латвія та Литва та багато інших [12].

Таким чином, в рамках ЄС інформаційна безпека розглядається, насамперед, як такий стан інформаційних мереж і систем, що забезпечує достатній рівень захисту цілісності, доступності, автентичності й конфіденційності інформації та належний рівень протидії зовнішнім негативним впливам. Пріоритетами політики країн ЄС в сфері інформаційної безпеки є створення і впровадження програм та різних технічних засобів захисту інформаційно-комунікаційних технологій; розробка нормативно-правових актів, які встановлюють перелік злочинів в ІТ-сфері та кримінальну відповідальність; забезпечення високого рівня обізнаності громадськості щодо ризиків, загроз та способів захисту своїх інформаційних систем/мереж від небажаних впливів.

Політика інформаційної безпеки на національному рівні реалізується державними органами влади та неурядовими організаціями. Урядові установи відповідають за розробку і координацію політики в сфері інформаційної безпеки. Втілення у життя державної політики належить до компетенції структурних підрозділів міністерств, комп'ютерними групами швидкого реагування на інциденти в сфері інформаційної безпеки та установами з питань захисту даних. З ініціативи або за підтримки державних органів влади в країнах ЄС реалізується низка інформаційно-освітніх та дослідницьких проектів, присвячених проблемі інформаційної безпеки. Роль неурядових організацій полягає, насамперед, в інформуванні громадськості про загрози і ризики в сфері інформаційної безпеки та способи захисту від них через розробку і реалізацію відповідних проектів, зокрема веб-сайтів, присвячених безпеці інформаційних технологій.

Список використаних джерел

1. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298 [Електронний ресурс].- Режим доступу: http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf
2. The European Network and Information Security Agency Електронний ресурс].- Режим доступу: http://www.enisa.europa.eu/
3. Safer Internet Programme [Електронний ресурс].- Режим доступу: http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm
4. Communication from the Commission: Towards a general policy on the fight against cyber crime. COM(2007) 267 [Електронний ресурс].- Режим доступу: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf
5. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009)149 [Електронний ресурс].- Режим доступу: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm
6. ENISA Country Reports 2009 [Електронний ресурс].- Режим доступу: http://www.epractice.eu/files/media/media2624.pdf
7. Finnish Ministry of Transport and Communications [Електронний ресурс].- Режим доступу: http://www.lvm.fi/web/en/home
8. CERT-Fi [Електронний ресурс].- Режим доступу: http://www.cert.fi/en/index.html
9. Estonian Cyber Security Strategy [Електронний ресурс].- Режим доступу: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf
10. Estonian Data Protection Inspectorate [Електронний ресурс].- Режим доступу: http://www.aki.ee/eng/
11. Computer Protection 2009 [Електронний ресурс].- Режим доступу: http://www.riso.ee/en/pub/2006it/docs/3.1.htm
12. Certification Centre of Estonia [Електронний ресурс].- Режим доступу: http://www.sk.ee/pages.php/0203