УДК 94(477)

Троян Сергій Станіславович,
доктор історичних наук, професор, професор кафедри міжнародних відносин, інформації та регіональних студій Національного авіаційного університету

ІНФОРМАЦІЙНО-БЕЗПЕКОВА ПОЛІТИКА ЄВРОПЕЙСЬКОГО СОЮЗУ

Інформаційна бомба розривається
в найбільшому скупченні людей,
осипаючи нас шрапнеллю образів
і докорінно змінюючи і сприйняття
нашого внутрішнього світу,
і нашу поведінку
(*Елвін Тоффлер*)

Анотація. *Інформаційна безпека займає важливе місце у політиці Європейського Союзу. Вона спрямована на захист інформаційних мереж і систем від негативних зовнішніх впливів і створення умов для безпечного функціонування особи, суспільства і держави в інформаційному просторі. Ключовими сегментами інформаційної політики ЄС є мережева та інформаційна безпека, а також протидія кіберзлочинності.*

Ключові слова: *інформаційна безпека, Європейський Союз, Європейська Комісія, кіберзлочинність, інформаційний простір.*

Аннотация. Троян С.С. Политика Европейского Союза в сфере информационной безопастности. *Информационная безопасность занимает важное место в политике Европейского Союза. Она направлена на защиту информационных сетей и систем от неблагоприятных внешних влияний и создание условий для безопастного функционирования личности, общества и государства в информационном пространстве. Ключевыми сегментами информационной политики ЕС являются сетевая и информацинная безопасность, а также противодействие киберпреступности.*

Ключевые слова: *информационная безопасность, Европейский Союз, Европейская Комиссия, киберпреступность, информационное пространство.*

Summary. Troyan Serhiy. European Union policy in the field of information security. *Information security occupies an important place in the policy of the European Union. It is aimed at protecting information networks and systems from negative external influences and creating conditions for the safe functioning of the individual, society and the state in the information space. The key segments of the EU information policy are network and information security as well as cybercrime counteraction.*

Key words: *information security, European Union, European Commission, cybercrime, information space.*

Вступ

Інформаційна безпека у межах Європейського Союзу розглядається, насамперед, як такий стан інформаційних мереж і систем, що забезпечує достатній рівень захисту цілісності, доступності й конфіденційності інформації та належний рівень протидії зовнішнім негативним впливам. Відповідно, одним з пріоритетів політики країн ЄС в сфері інформаційної безпеки є розробка і впровадження програм та різних технічних засобів, які дозволяють підтримувати певний рівень захисту інформаційно-комунікаційних технологій.

Поряд з цим, значна увага в рамках ЄС приділяється правовим засадам інформаційної безпеки, що передбачає розробку нормативно-правових актів, які б встановлювали перелік злочинів, пов’язаних із інформаційними технологіями, й визначали відповідну кримінальну відповідальність.

Іншим пріоритетом політики ЄС є інформаційна безпека громадян. По суті це високий рівень обізнаності громадськості щодо ризиків та загроз, пов'язаних з інформаційними технологіями, та щодо способів захисту своїх інформаційних систем/мереж від небажаних впливів. Сюди відноситься не лише протидія кібератакам, але й захист персональних даних, виявлення шкідливого контенту в мережі Інтернет тощо.

Мережеві й інформаційні аспекти безпеки в контексті інформаційної політики ЄС

Початок інформаційної політики ЄС пов'язують з проголошенням у 1994 році доктрини Європейського інформаційного суспільства, відомої як доповідь Мартіна Бангемана «Європа і глобальне інформаційне суспільство: рекомендації для Європейського Союзу» [13]. Базові ідеї документу були спрямовані на створення інформаційного суспільства на основі процесу європейської інтеграції для забезпечення економічної стабільності країн Європи; розв'язання актуальних соціальних проблем; надання можливостей для вільного доступу до глобальних мереж із метою освіти, охорони здоров'я та адміністративного управління. На основі усвідомлення перспективної значимості нових тенденцій інформаційного розвитку Європейська Комісія в тому ж 1994 році прийняла програмний документ «Шлях Європи до інформаційного суспільства». Сформульовані там основні принципи діяльності ЄС в галузі інформації і комунікації полягали в необхідності формування суспільної думки та підготовці європейської спільноти до усвідомлення реалій інформаційного суспільства; у створенні концепції європейської інформаційної політики; у забезпеченні вільного доступу до інформаційних послуг; впровадження багатомовності в інформаційній і комунікаційній діяльності, збереженні національної культурної самобутності та ідентичності тощо.

Загальну політика в галузі інформації та комунікації Європейський Союз реалізує через свої основні органи та спеціалізовані структури. Насамперед йдеться про Європейську Раду, Європейську Комісію, Генеральний Директорат з інформаційного суспільства, Форум інформаційного суспільства ЄС, Генеральний Директорат з освіти і культури та про інформаційні центри як у країнах-членах організації, так і за її межами.

На сучасному етапі особливого значення для держав ЄС набувають питання мережевої та інформаційної безпеки. Європейські фахівці в галузі інформаційних систем, безпеки і стратегічного планування активно обговорюють проблеми, що виникають перед державами Європейського Союзу в умовах можливості застосування інформаційної зброї, тобто засобів спрямованого впливу на інформаційні ресурси ймовірного супротивника у військовий і мирний час. Сьогодні на практиці реалізуються плани організаційного та технічного забезпечення національної інформаційної безпеки, створюються підрозділи, призначені для відбиття «інформаційної агресії». Уряди беруть на себе роль координаторів міжвідомчих зусиль у цій сфері.

Крім вивчення технічних аспектів інформаційної безпеки, у Західній Європі активізувалася робота з оцінки впливу інформації на особистість і суспільство. При цьому робиться наголос на визначення методів та засобів надання «інформаційної протидії», каналів впливу на людину, впливу тієї чи іншої інформації на боєздатність збройних сил, дослідження взаємин ЗМІ та суспільної думки [4; 6; 7; 9].

Розробка методів і засобів забезпечення інформаційної безпеки відбувається в Західній Європі за такими основними напрямками: 1) виявлення загрози нападу, 2) нейтралізація нападу, 3) захист і 4) відновлення власних систем.

У 2001 році Європейською Комісією було представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід» (Network and Information Security: Proposal for A European Policy Approach), в якому окреслено європейський підхід до проблеми інформаційної безпеки [3].

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.

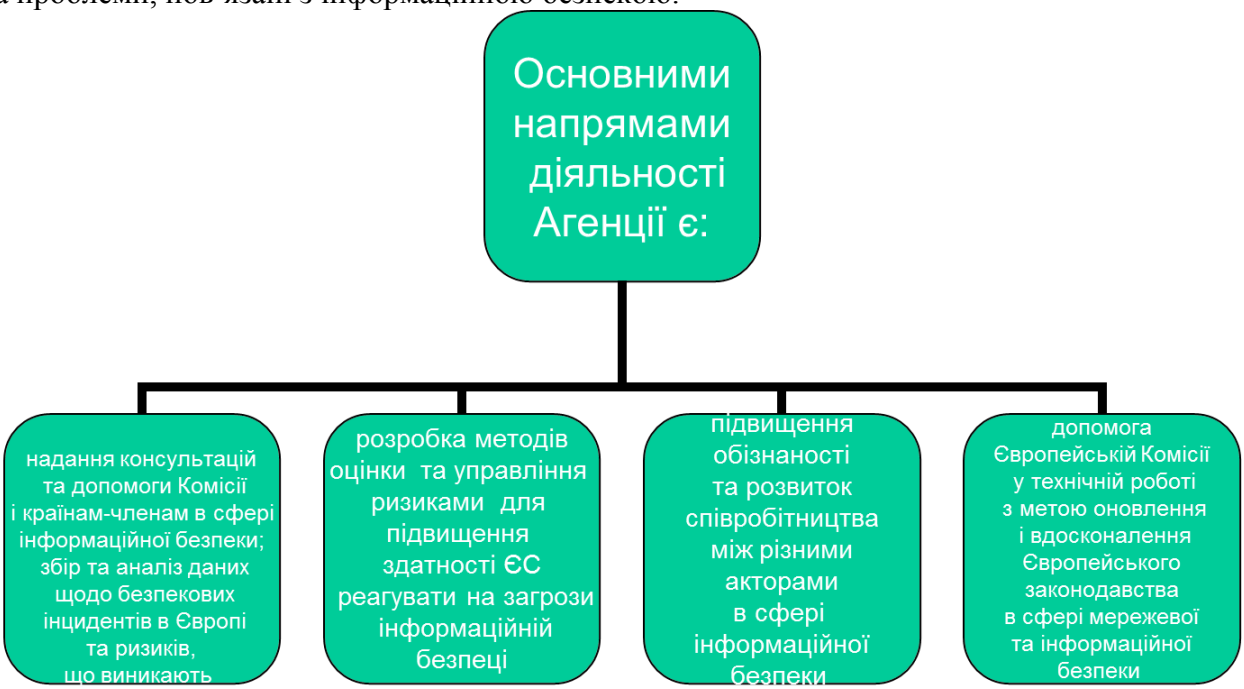
«Мережева та інформаційна безпека: європейський політичний підхід» визначив такі основні напрями європейської політики інформаційної безпеки:

- підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;
- створення європейської системи попередження та інформування про нові загрози;
- забезпечення технологічної підтримки;
- підтримка ринково орієнтованої стандартизації та сертифікації;
- правове забезпечення ;
- зміцнення безпеки на державному рівні;
- розвиток міжнародного співробітництва з питань інформаційної безпеки.

На сьогодні Європейська Комісія бере участь у роботі Великої Сімки, Організації економічного співробітництва і розвитку та ООН. Приватний сектор працює над проблемами безпеки в таких організаціях як Глобальний бізнес-діалог (www.GBDe.org) або Глобальний Інтернет-проект (www.GIP.org).

Основне завдання ЄС – подальше 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). Це спеціалізована агенція ЄС, 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.



З 2007 року ENISA підтримує проекти співробітництва між країнами-членами ЄС в сфері інформаційної безпеки. Так, ENISA надала підтримку проектам співпраці між Угорщиною та Болгарією щодо створення Болгарської урядової комп’ютерної групи швидкого реагування (CERT), а також співробітництва між CERT-FI (Фінляндія) та CSIR/MERAKA (Південна Африка) щодо обміну досвідом та створення Південно-Африканської групи реагування на комп’ютерні інциденти (Computer Security Incident Response Team).

ENISA також сприяла розвитку партнерства між приватними і державними структурами щодо обміну інформацією про кіберзлочини між фінансовим сектором і державними органами через Центри фінансової інформації та аналізу (FI-ISAC). У 2008-2009 роках Агенцією створено структуру/систему, що допомагає зацікавленим сторонам краще ідентифікувати та розуміти поточні та майбутні ризики (Emerging and Future Risks), породжені новітніми інформаційними технологіями. Агенцією започатковано також Форум з безпекових питань та створено експертні групи, які дають оцінку та аналізують відповідні проблеми.

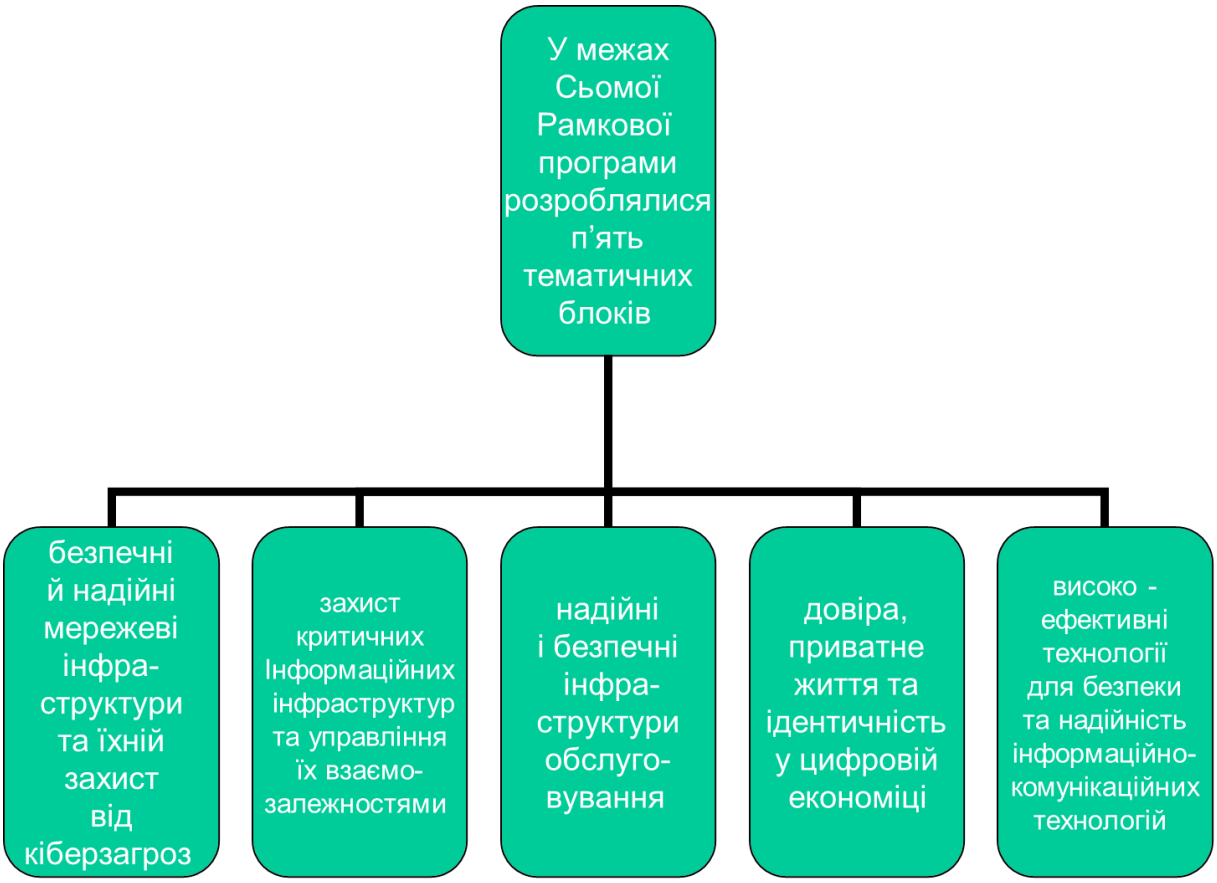
Проблема інформаційної безпеки були одним з пріоритетів Сьомої Рамкової програми ЄС (2007-2013 рр.) [3]. Дослідження з безпеки інформаційно-комунікаційних технологій в Сьомій Рамковій Програмі спрямовані на розвиток знань і технологій для розбудови відкритого, безпечного інформаційного суспільства в Європі, в якому громадяни та організації можуть повною мірою користуватися перевагами нових технологій.

Основний акцент зроблено на підвищенні можливостей користувачів управляти і захищати свої цифрові засоби, ідентичність та персональні дані у цифровому середовищі. Ще у 1995 році була прийнята директива про захист персональних даних у Європейському Союзі. Вона закріплювала два основних права:

а) право на захист персональних даних;

б) право на вільне поширення персональних даних.

У 2002 році була прийнята ще одна директива про недоторканність приватного життя й електронних даних і носіїв інформації.



У 2008 році розпочато реалізацію 33-х дослідницьких проектів з проблеми безпеки і довіри в інформаційному суспільстві. Бюджет складає понад 160 мільйонів євро.

Значна увага в рамках ЄС приділяється проблемі кібербезпеки як складової інформаційної безпеки (*про це – див. далі*).

З 1999 року ЄС реалізує програми «Безпечніший Інтернет» (Safer Internet). Тривалість кожної програми – 4-5 років. В рамках програми "Безпечніший Інтернет" фінансується низка

проектів. Перш за все, це Інтернет-центри, які створюються на національному рівні і координуються на європейському рівні. Основна мета діяльності центрів – підвищення обізнаності дітей, батьків, вчителів про онлайн ризики, а також надання порад молоді щодо безпечного користування мережею через телефони довіри та контактні пункти. Такі Інтернет-центри функціонують у 28 країнах-членах ЄС [3; 11].

Для боротьби з незаконним контентом в рамках програми фінансуються такі проекти, як CIRCAMP – тематична мережа для розвитку міжнародного співробітництва правоохоронних органів; База даних Інтерполу про акти сексуального насильства над дітьми (INTERPOL International Child Sexual Exploitation Image Database), мета якої полягає у попередженні та виявленні актів сексуального насильства над дітьми через ідентифікацію жертв та зловмисників тощо.

На сучасному етапі функціонування та розвитку мережевого сегменту інформаційного суспільства в державах ЄС важлива роль відводиться програмі «Горизонт 2020» [1]. Це найбільша в історії Європейського Союзу програма, спрямована на фінансування досліджень та інновацій, із загальним бюджетом близько 80 млрд. євро, розрахованим на сім років (2014 – 2020) . Вона прийшла на зміну 7-й Рамковій програмі ЄС з досліджень і технологічного розвитку (7РП), що діяла з 2007 по 2013 роки. Програма «Горизонт 2020» покликана сприяти збільшенню числа передових технологій, відкриттів і перспективних розробок шляхом просування ідей з наукових лабораторій до ринку. Заснована на трьох ключових пріоритетах – передовій науці, лідерстві у промисловості та суспільних викликах – програма надає підтримку широкому спектру діяльності, від наукових досліджень до демонстраційних проектів та інновацій, готових до виходу на ринок.

Інформаційна політика ЄС у сфері протидії кіберзлочинності

Вагоме місце у контексті еволюції мережевого і безпекового виміру інформаційного суспільства Європейського Союзу посідає боротьба з кіберзлочинністю [12]. Поняття «кіберзлочинність» вперше з'явилось в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних.

Найпоширеніша класифікація кіберзлочинів ґрунтується на Конвенції Ради Європи про кіберзлочинність, що була відкрита для підписання у листопаді 2001 р. В цьому документі кіберзлочини поділяються на п'ять груп:

I – злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему);

II – злочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів, тобто для маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерні підроблення);

III – злочини, пов'язані з контентом (змістом даних);

IV – злочини, пов'язані з порушенням авторського права і суміжних прав;

V – акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж [5; 10].

У травні 2007 році Європейською Комісією було представлено документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» (Towards a general policy on the fight against cyber crime), в якому дається визначення терміну «кіберзлочинність» та висвітлено основні напрями політики ЄС в сфері боротьби з кіберзлочинністю.

Кіберзлочинність – це кримінальні дії, скоєні з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем. Характерною рисою кіберзлочинів є масовий масштаб та значна географічна відстань між самим злочином і його наслідками.

Політика Європейської Комісії в сфері боротьби з кіберзлочинністю реалізується за чотирма основними напрямами.

По-перше, це участь у законодавчому процесі. Найважливішим 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. Сюди відноситься хакерство, DoS-атаки, поширення шкідливого коду, шпигунських програм та вірусів. Згідно з рішенням покарання за незаконне втручання у систему та незаконна модифікація, пошкодження або знищення даних має складати щонайменше 2-3 роки тюремного ув'язнення. Підбурювання, надання допомоги, співучасть та спроби вчинити вище зазначені злочини також мають кваліфікуватися країнами-членами як кримінальні злочини.

По-друге, Європейська Комісія заохочує транскордонне співробітництво правоохоронних органів країн-членів ЄС. В рамках цього напряму діяльності здійснюються такі заходи:

- організація конференцій з питань кіберзлочинності,
- створення цілодобових контактних пунктів у країнах-членах ЄС,
- розвиток 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. Так, у 2007 році Комісією було організовано зустріч експертів державних і приватних установ, на якій обговорювалося питання розвитку співпраці між цими спеціалістами в рамках ЄС.

По-четверте, Європейська Комісія відіграє координуючу роль на міжнародному рівні: заохочує підписання країнами-членами та іншими країнами Конвенції про кіберзлочинність, розробленої Радою Європи, та бере участь у міжнародних робочих групах [3].

У березні 2009 року опубліковано Повідомлення Європейської Комісії під назвою «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» (Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience). У Повідомленні 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.

Згідно з Повідомлення Європейської Комісії «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості», сьогодні 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 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 організація тренінгів для широкомасштабного реагування на безпекові інциденти; проведення панєвропейських навчань з проблеми безпекових інцидентів в 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 [3; 11].

У листопаді 2010 року Європейська Комісія прийняла Стратегію внутрішньої безпеки ЄС на 2011 – 2014 рр. Вона передбачала реалізацію п'яти стратегічних цілей для піднсення ефективності у сфері запобігання і протидії організованій злочинності, тероризму, радикалізації, кіберзлочинності, охорони кордонів. 25 жовтня 2011 року Європейський Парламент прийняв резолюцію щодо організованої злочинності в ЄС і важливості протидії її згубним впливам на євроспільноту [14]. У 2012 році в рамках Європарламенту було створено тимчасовий Спеціальний комітет з питань протидії організованій злочинності, корупції та відмивання брудних грошей (CRIM).

Протидія кіберзлочинності займає важливе місце для ЄС в контексті реалізації програми «Східного партнерства» [8]. ЄС запропонував усім країнам-партнерам до 2020 року схвалити Стратегію або Плани дій щодо вирішення проблем із кіберзлочинністю, створити повноцінні діючі підрозділи по боротьбі з цим явищем та повністю імплементувати Будапештську Конвенцію з протидії кіберзлочинності.

Україна вже досягла зазначених цілей – Планом заходів на 2017 рік з реалізації Стратегії кібербезпеки України передбачено імплементацію Конвенції про кіберзлочинність і відповідної Директиви 2008/114/ЄК та наближення законодавства України до законодавства ЄС у цій сфері. В Україні діють Національний координаційний центр кібербезпеки в РНБОУ, Департамент кіберполіції Національної поліції України (з 2015 р.), спеціалізований підрозділ з кібербезпеки СБУ і CERT-UA при Держспецзв'язку.

Хоча у першій редакції Спільного робочого документа ЄС «протидія гібридним загрозам» не була відображена, але вже у нинішній редакції Євросоюз визначив відповідні цілі до 2020 року і зробив акцент на захист критичної інфраструктури та кібербезпеку.

Для України ці сфери є вкрай важливими. Так, кіберпростір українські експерти, які взяли участь в опитуванні в рамках проекту «Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз» за підтримки проекту «Громадська синергія», назвали одним з головних напрямків основного удару для ведення війни гібридного характеру РФ проти України.

У контексті протидії кіберзлочинності на перспективу відзначимо, що з 2018 року в ЄС почали діяти суворіші закони щодо захисту персональних даних. В цьому плані фахівці радять організаціям, які збирають дані такого рівня, мати окремого спеціаліста, відповідального за їх захист. На основі реалізації нової стратегії розвитку інформаційного простору [2] Європейський Союз має чіткий намір зміцнити в ньому свої позиції, зокрема і в сенсі мережевої та інформаційної безпеки і протидії кіберзлочинності.

Висновки

1. 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.

2. Експерти провідних держав Європейського Союзу дійшли висновку, що у зв'язку зі зростанням значимості інформаційного чинника для прийняття рішень на урядовому, військовому і промисловому рівнях необхідна диверсифікованість джерел одержання даних, а також механізмів їхньої обробки та способів доведення до споживачів.

3. У державах і структурах Європейського Союзу підкреслюється важливість наявності національних інформаційних агентств із незалежною мережею кореспондентів, що дозволить виявляти дезінформацію, здатну впливати на прийняття державних рішень. Висуваються ідеї створення баз даних за джерелами інформації (наукові установи, ЗМІ, приватні особи) для одержання достовірних і оперативних відомостей (із конфіденційних джерел) у кризових ситуаціях.

4. У Європейському Союзі слідом за політичною інтеграцією почалось фактичне об'єднання у сфері інформаційних ресурсів. Це має своїм головним наслідком формування єдиного інформаційного простору.

5. Наявність єдиного інформаційного простору призвело до залежності окремих держав від інформаційних потоків, котрі охоплюють суспільство. Таким чином, вплив на ці потоки з метою псування, перекручування інформації, що знаходиться в них, а також виводу з ладу інформаційних інфраструктур переростає в Європі з національної проблеми в міжнародну і вимагає подальшого розвитку скоординованої політики в сфері забезпечення інформаційної безпеки.

Джерела і література

1. Горизонт 2020: Рамкова програма ЄС з досліджень та інновацій [Електронний ресурс]. – Режим доступу: https://new.kmu.gov.ua/storage/app/media/uploaded-files/broshura-gorizont-2020-1201.pdf (доступ – 19 грудня 2017 р.).
2. ЄС представив нову стратегію розвитку інформаційного простору [Електронний ресурс]. – Режим доступу: https://www.rbc.ua/ukr/news/es-predstavil-novuyu-strategiyu-razvitiya-1430943131.html (доступ – 19 грудня 2017 р.).
3. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки // Актуальні проблеми міжнародних відносин: зб. наук. пр. / Київський нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. – К., 2009. – Вип. 87, ч. 2. – С. 36-45.
4. Информационно-психологическая безопасность в эпоху глобализации [Текст]: учеб. пособ. / В.М. Петрик, В.В. Остроухов, А.А. Штоквиш и др.; под ред. В.В. Остроухова. – К.: МОО «Международное антитеррористическое единство», 2008. – 544 с.

5. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/994_575 (доступ – 19 грудня 2017 р.).
6. Кузьменко А. Інформаційно-психологічна війна епохи глобалізації (Частина 2. Доктринальні підходи Європейського союзу, ФРН і Французької Республіки) // Юридичний журнал. – 2007. – № 6. – http://www.justinian.com.ua/article.php?id=2662 (доступ – 19 грудня 2017 р.).
7. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны – 2-е изд., стереотип. – М.: Горячая линия. Телеком, 2006. – 541 с.
8. Мартинюк В. Безпека для Східного партнерства: які зміни варто лобіювати Україні [Електронний ресурс]. – Режим доступу: http://www.eurointegration.com.ua/articles/2017/11/20/7073879/ (доступ – 19 грудня 2017 р.).
9. Міжнародна інформаційна безпека: теорія та практика / Є.А. Макаренко, М.М. Рижков, М.А. Ожеван та ін. – К.: Видавничий дім Lat&K, 2012. – 350 с.
10. Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. – 2013. – № 5 – С. 148-160.
11. Тихомирова Є.Б. Комунікативна політика ЄС: інформаційна безпека vs транспарентність // Актуальні проблеми міжнародних відносин: зб. наук. пр. / Київський нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. – К., 2011. – Вип. 102, ч. 1. – С. 22-28.
12. Шостко О.Ю. Протидія організованій злочинності в європейських країнах: монографія. – Х.: Право, 2009. – 400 с.
13. Bruggemann M. Information policy and the public sphere: EU communications and the promises of dialogue and transparency // Javnost – The Public, Journal of the European Institute for Communication and Culture. – Vol. 17. – 2010. – № 1. – P. 5-22.
14. European Parliament resolution of 25 October 2011 on organised crime in the European Union [Електронний ресурс]. Режим доступу: http://www.europarl.europa.eu/sides/getDoc.do?type= TA&reference=P7-TA-2011-0459&language=EN (доступ – 19 грудня 2017 р.).