Інформатизація та інформаційна безпека

УДК:343.5:004

КУРЕНДА Л.Д., *кандидат педагогічних наук*, доцент кафедри теорії та історії держави і права Волинського національного університету імені Лесі Українки

ОКРЕМІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Анотація. *У науковій статті проводиться аналіз теоретико-правових засад формування основних концепцій забезпечення інформаційної безпеки Європейського Союзу.*

Аннотация. *В научной статье проводится анализ теоретико-правовых принципов формирования основных концепций обеспечения информационной безопасности Европейского Союза.*

Summary. *In the scientific article the detailed analysis is conducted teoretiko-legal principles of forming of basic conceptions of providing of informative safety of European Union.*

Ключові слова: *інформація, безпека, Європейський Союз, Інтернет, персональні дані.*

Постановка проблеми. Проблема забезпечення інформаційної безпеки Європейського Союзу (надалі – ЄС), розглядається поряд з іншими проблемами становлення інформаційного суспільства. Зауважимо, що аналіз низки нормативно-правових актів та планів дій у сфері становлення інформаційного суспільства ЄС, дозволив дійти висновку про значно вужче розуміння поняття “інформаційна безпека” як щодо українського, так і до міжнародного законодавства. Забезпечення інформаційної безпеки було визнано глобальною проблемою сучасності відповідно до Резолюції 54/49 ООН “Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” від 1 грудня 1999 року [1]. Представники різних країн наголошували, що використання нових інформаційних технологій і засобів впливу високорозвинених країн на менш технологічні країни світу призвело до зміни глобального і регіонального балансів сили, обумовило нові сфери конфронтації між традиційними і новими центрами глобального протистояння, уможливило досягнення переваг в інформаційних технологіях і засобах маніпулювання суспільною свідомістю для широкомасштабної експансії із застосуванням не обмежених міжнародним правом видів озброєнь [2]. Отже, актуальність таких проблем, як інформаційно-технологічний дисбаланс, інформаційна ізоляція окремих регіонів, країн, а також негативний вплив інформаційних технологій, акцентується не тільки ЮНЕСКО, а й іншими міжнародними організаціями, зокрема ООН.

Аналіз останніх досліджень і публікацій. Проблема теоретико-правових засад забезпечення інформаційної безпеки ЄС у вітчизняній науковій літературі достатньо ґрунтовно не досліджувалась. Вона розглядалася лише через висвітлення окремих її аспектів вітчизняними та зарубіжними фахівцями інформаційного права, національної безпеки, а саме: С.С. Алексєєв, І.Л. Бачило, К.І. Бєляков, В.Т. Білоус, В.Д. Гавловський, В.О. Голубєв, М.В. Гуцалюк, О.П. Дубас, Р.А. Калюжний, А.М. Колодій, В.О. Копилов, В.А. Ліпкан, В.В. Макаренко, Є.А. Макаренко, Н.Р. Нижник, В.М. Петренко, П.М. Рабінович, А.О. Селіванов, М.Я. Швець, Ю.С. Шемшученко, О.К. Юдін, В.І. Ярочкін та інші.

Метою статті є проведення аналізу теоретико-правових засад формування основних концепцій забезпечення інформаційної безпеки Європейського Союзу.

Виклад основних положень. З огляду на глобальність та актуальність процесу забезпечення інформаційної безпеки в інформаційному столітті, держави-члени ООН виробили єдину термінологію та узгодили зміст основних понять в інформаційній сфері міжнародного співробітництва.

Так, “міжнародна інформаційна безпека” визначається як взаємодія акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційних загроз.

“Інфосфера” – міжнародний інформаційний простір, що складається з інформаційних потоків, інформаційних ресурсів та всіх сфер життєдіяльності цивілізації.

Беручи до уваги вказану дефініцію, можна дійти висновку, що забезпечення міжнародної інформаційної безпеки охоплює три аспекти:

- інформаційно-технічний (“захист глобальної інфраструктури”);
- інформаційно-психологічний (“захист суспільної свідомості світової спільноти”);
- інформаційну безпеку у сфері прав та свобод (“захист міжнародної інфосфери”).

Таким чином, позиція українського законодавця (Закон України “Про основи національної безпеки України”) цілковито відповідає стандартам міжнародної спільноти, де на підставі переліку загроз національній безпеці України в інформаційній сфері, ми умовно виокремили такі ж аспекти інформаційної безпеки України. Отже, українська дефініція є більш повною та досконалою щодо європейського визначення поняття “інформаційної безпеки”, яке охоплює тільки інформаційно-технічний аспект.

На наш погляд, досить вдалим для розкриття предмета дослідження є аналіз науково-практичної літератури з проблем міжнародної інформаційної політики, зроблений Є.А. Макаренко, на підставі якого дослідник виокремив чотири моделі глобальної (міжнародної) інформаційної безпеки.

Модель А – створення абсолютної системи захисту країни-інфолідера проти будь-якого виду наступальної інформаційної зброї, що зумовлює об’єктивні переваги у потенційній інформаційній війні, змушує інші країни шукати альянсу щодо військово-інформаційних діях з країною-інфолідером. При цьому може бути використано систему жорсткого контролю над інформаційним озброєнням противника на підставі потенційних міжнародних документів з інформаційної безпеки.

Модель В – створення значної переваги держави – потенційного ініціатора інформаційної війни у наступальних видах озброєнь, знешкодженні систем захисту держави-противника засобами інформаційного впливу, координація дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації будь-яких джерел і типів інформаційних загроз.

Модель С – наявність кількох країн – інфолідерів та потенційного протиборства між ними, визначення фактора стримування експансії інформаційних загроз, забезпечення у перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світопорядку.

Модель D – усі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів, досягнення переваг локальних рішень, спроможних заблокувати технологічне лідерство, використання можливостей

інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами (політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій [3, с. 204].

Отже, міжнародне співтовариство визнає, що боротьба та протиборство між країнами на сьогодні здійснюється переважно з використанням інформаційної зброї, що зумовлює інформаційний характер загроз та небезпек.

У зв’язку з цим міжнародна спільнота термінологічно узгодила інші важливі поняття. Так, під “інформаційною війною” слід розуміти інформаційне протиборство з метою впливу на критично важливі структури противника, зруйнування політичної та соціальної систем, а також для дестабілізації суспільства і державності противної сторони. “Інформаційна зброя”, у свою чергу, визначається як комплекс технічних та інших заходів, методів і технологій, спрямованих на встановлення контролю над інформаційними структурами потенційного противника, втручання у роботу його систем управління, інформаційних мереж та комунікацій з метою знищення або модифікації даних, дезінформації, поширення інформації спеціального призначення у системах формування громадської думки і прийняття рішень, а також як сукупність засобів впливу на свідомість і психологічний стан політичних та військових структур, спецслужб і населення для протидії можливим інформаційним впливам іншої сторони.

Використовуючи як джерело інформації офіційний сайт ЄС, де в підрозділі, присвяченому питанню становлення інформаційного суспільства ЄС, є пункти, що конкретизують проблему інформаційної безпеки ЄС, зокрема:

- безпека використання Інтернету (“Safer Internet plus (2005-2008)”, “Safer Internet (1999-2005)”);
- безпека мережі (атаки на інформаційні системи, боротьба з кіберзлочинами);
- захист персональних даних (у межах даного пункту є підпункт під назвою “інформаційна безпека”).

При розкритті позиції ЄС у сфері забезпечення безпеки інформаційного суспільства поряд із зазначеними вище проблемами, також приділяється увага іншим проблемам інформаційного характеру – електронна торгівля, використання інформаційних технологій для дорожньої безпеки, безпека радіозв'язку та телекомунікацій тощо. Наприклад, електронна торгівля ЄС урегульована Директивою ЄС “Про деякі правові аспекти інформаційних послуг, зокрема електронної комерції, на внутрішньому ринку” (“Директива про електронну комерцію”) від 8 червня 2000 року. Щодо українського законодавства, то на сьогодні не існує окремого нормативно-правового акту, що регулює суспільні відносини у сфері електронної торгівлі.

З огляду як на позитивну, так і негативну роль глобальної мережі Інтернет у становленні глобального та європейського інформаційного суспільства, особливої актуальності набуває проблема безпеки цієї мережі.

Єврокомісія прийняла Резолюцію про запобігання поширенню в Інтернет інформації незаконного змісту, шкідливої для морального здоров’я суспільства в 1996 році, відповідно до якої поняття шкідливого змісту залежить від культурних традицій, а поняття “незаконного змісту” – від чинного законодавства [4].

Згідно з цією Резолюцією, основними заходами для забезпечення безпеки інформації в мережі Інтернет є:

1) забезпечення свободи комунікації он-лайн;

2) визначення обов’язків постачальників послуг (зокрема, видавців та посередників);

3) запровадження захисту інтелектуальної власності в режимі он-лайн;

4) забезпечення ефективного регулювання змісту інформації, що є в мережі Internet;

5) забезпечення захисту персональних даних;

6) забезпечення правового статусу доменів;

7) забезпечення вільного доступу до масивів інформації в мережі Інтернет для масового використання (досвід Франції) [3, с. 232].

Зауважимо, що для забезпечення безпеки Інтернету, Європейський Союз розробив плани дій.

Так, План дій “Безпечний Інтернет (1999 – 2005)” – це план дій, головною метою якого є створення сприятливішого середовища для розвитку Інтернет-промисловості, шляхом безпечного використання Інтернету та боротьби з незаконним або шкідливим змістом. Спочатку виконання цього Плану було розраховано на період з 1999 року до 2002 року, але наприкінці травня 2003 року, Рада ЄС погодилася з Європейським парламентом щодо необхідності розширення цього Плану ще на два роки.

Для реалізації проголошеної мети, План передбачає виконання таких завдань:

1) установлення безпечного середовища через європейську мережу “екстрених зв’язків” та, заохочувальну саморегуляцію та кодекси поведінки;

2) розвиток фільтруючих та оцінюючих інструментів, особливо тих, що відповідають міжнародним стандартам щодо оцінки таких систем;

3) проведення кампаній з метою допомоги особам, що мають справу з дітьми на всіх рівнях, кращого способу захисту дітей від шкідливої інформації;

4) координація та взаємодія Європейського Союзу з міжнародним співтовариством у цій сфері.

Відповідно до цих завдань та поставленої мети, План-дій “Безпечний Інтернет (1999 – 2005)” передбачає виконання таких заходів:

1) контроль за змістом інформації (особливо інформації, пов’язаної з дитячою порнографією, расизмом, антисемітизмом тощо);

2) створення таких механізмів, що дозволять допомогти батькам та викладачам, контролювати зміст інформації, до якої мають доступ діти;

3) надання послуг, спрямованих на отримання дорослими та дітьми більших знань щодо можливостей Інтернету;

4) міжнародне співробітництво у цій сфері.

Новий План-дій “Більш безпечний Інтернет Плюс (2005 – 2008)” було прийнято у квітні 2005 року як продовження Плану дій “Безпечний Інтернет (1999 – 2005)” та, спрямований не лише на безпечніше використання Інтернету, а й нових технологій он-лайн та захисту користувача від небажаного і шкідливого Інтернет-змісту.

Згідно з Планом-дій “Безпечний Інтернет плюс (2005 – 2008)”, основними завданнями для реалізації цієї мети є:

1) боротьба з незаконним змістом інформації шляхом розширення “екстрених зв’язків” до міжнародного рівня та обміну інформацією і досвідом з іншими країнами;

2) боротьба з небажаним та шкідливим змістом шляхом використання технологічних досягнень;

3) просування більш безпечного навколишнього середовища шляхом створення Інтернет-форуму;

4) захист даних та споживача шляхом забезпечення інформаційної і мережевої безпеки від вірусів та ін.

Наступною проблемою є забезпечення “безпеки мережі”, що охоплює розгляд таких питань:

- атаки на інформаційні системи;
- боротьба з кіберзлочинами.

Відповідно до Рішення Ради ЄС “Про атаки на інформаційні системи” від 24 лютого 2005 року під атаками на інформаційні системи розуміється:

1) незаконний доступ до інформаційних систем;
2) незаконне втручання в інформаційні системи (навмисне серйозне перешкоджання чи переривання функціонування інформаційної системи);
3) незаконне втручання в комп’ютерні дані [5].

У свою чергу, під інформаційними системами розуміють будь-який пристрій чи групу пристроїв, що виконують автоматичну обробку комп’ютерних даних.

Зазначається, що у всіх випадках злочинна дія повинна визнаватися навмисною. Підбурювання, допомога, співучасть у згаданих злочинних діях є так само кримінально караним діянням.

У рамках безпеки мережі виокремлюється проблема боротьба з кіберзлочинами. Боротьба з кіберзлочинністю є особливо актуальною проблемою для країн Європи, що зумовлено високим рівнем комп’ютерної оснащеності різних сфер життєдіяльності суспільства.

Так, на сайті Євросоюзу зауважується, що створення більш безпечного інформаційного суспільства шляхом безпеки інформаційної інфраструктури зумовлює боротьбу з комп’ютерними злочинами.

Взагалі, як зазначає І.В. Арістова, у найбільш розвинених країнах світу розробка правових заходів у боротьбі з комп’ютерною злочинністю і захисту інформаційного простору ведеться вже понад двадцять років. З метою уніфікації національних законодавств Рада Міністрів Європейського Союзу в 1989 р. розробила список правопорушень у сфері комп’ютерної інформації, рекомендований державам-членам ЄС для створення кримінально-правової стратегії розробки законодавства [6, с. 178].

Боротьба з комп’ютерною злочинністю має доволі потужну нормативно-правову основу.

Статті 29 і 34 Договору про заснування Європейського Союзу, Директива Парламенту і Ради 95/46/ЕС “Про захист фізичних осіб у зв’язку з обробкою персональних даних та вільного обігу цих даних” від 24 жовтня 1995 року; Регламент Парламенту і Ради ЄС № 45/2001 “Про захист фізичних осіб у зв’язку з обробкою персональних даних інституціями і органами Співтовариства та про вільний обіг цих даних” від 18 грудня 2000 року, Резолюція Ради ЄС “Про законний моніторинг телекомунікацій” від 17 січня 1995 року – це лише частина нормативно-правових актів Європейського Союзу, що порушують питання боротьби з комп’ютерною злочинністю.

Слід зауважити, що Європейський Союз лише готується до імплементації Конвенції Ради Європи “Про кіберзлочинність” від 23 листопада 2001 року, який є базовим міжнародним нормативно-правовим актом, що регулює суспільні відносини у сфері протидії кіберзлочинам. Першими кроками на цьому шляху були Спільна Позиція 1999/364/JHA від 27 травня 1999 року, затверджена Радою ЄС на підставі ст. 34 Договору про заснування ЄС щодо переговорів проекту Конвенції про комп’ютерну злочинність, які відбулися у Раді Європи, та Пропозиції для Рамкового Рішення Ради ЄС щодо атак, спрямованих на інформаційні системи.

На сайті Євросоюзу зазначається, що під комп’ютерним злочином в найширшому розумінні є будь-який злочин, пов’язаний з використанням інформаційних технологій. Терміни “комп’ютерний злочин”, “злочин на основі високих технологій” та “кіберзлочин” є синонімічними.

Євросоюз виокремлює чотири групи комп’ютерних злочинів, а саме:

1) злочини таємності: незаконний доступ, збереження, модифікація, розкриття або поширення анкетних даних;

2) комп’ютерні злочини, пов’язані зі змістом: поширення порнографії, дитячої зокрема, расистської та насильницької інформації;

3) економічні злочини: незаконний доступ до систем (наприклад, комп’ютерне шпигунство, підробка, шахрайство тощо);

4) злочини інтелектуальної власності: порушення юридичного захисту комп’ютерних програм та баз даних, авторського права та суміжних прав.

Саме така класифікація комп’ютерних злочинів передбачена Конвенцією Ради Європи “Про кіберзлочинність”.

З метою підвищення спроможності ЄС забезпечити мережеву та інформаційну безпеку, було створено Європейське агентство мережевої та інформаційної безпеки (ENISA) у 2004 році, головними завданнями якої є:

1) збір інформації з метою аналізу потенційних інформаційних ризиків та повідомлення про них держав-учасниць;

2) збільшення співробітництва на всіх рівнях з метою ознайомлення досвідом у сфері мережевої та інформаційної безпеки;

3) відстеження розвитку стандартів у сфері безпеки послуг і продуктів та ознайомлення з ними країн-учасниць.

Як зазначалося вище, на сайті Європейського Союзу в межах підпункту “безпека мережі” (“network security”), під мережевою та інформаційною безпекою розуміється здатність мережі або інформаційної системи, протистояти випадковим подіям або незаконним чи зловмисним діям, що ставлять під загрозу придатність, дійсність, цілісність і конфіденційність збережених або переданих даних та пов’язаних з цим послуг.

Оскільки в інформаційному суспільстві кожний громадянин країн-учасниць ЄС має право доступу до даних відкритого характеру (закони, урядові рішення, інформація засобів масової комунікації), культурної спадщини (літературні твори, не обмежені авторським правом і віднесені до національного надбання, наукові праці, безоплатне програмне забезпечення, непатентовані стандарти), а також до інформації відкритого характеру в комп’ютерних мережах і системах, що потребує осмислення відповідальності за здійснення нової політики [7], серйозною проблемою для Євросоюзу є захист персональних даних.

Варто погодитись із Ю.Є. Максименко, яка зазначає, що: 1) глобальність проблеми забезпечення інформаційної безпеки потребує інтенсифікації міжнародного співробітництва у цій сфері; 2) визначення поняття “інформаційна безпека Європейського Союзу” має значно вужче розуміння щодо міжнародних стандартів та українського законодавства, ототожнюючи інформаційну безпеку з інформаційно-технічною, залишаючи осторонь інші складові — інформаційно-психологічну та інформаційну безпеку у сфері прав і свобод людини та громадянина; 3) відсутність нормативної дефініції “інформаційна безпека ЄС”, зумовлює неоднозначне трактування її змісту, що ускладнює узгодження правових норм у сфері забезпечення інформаційної безпеки; 4) більш високий рівень розвитку інформаційної інфраструктури ЄС щодо України зумовлює наявність нормативного регулювання суспільних відносин (наприклад, у сфері електронної комерції, використання інформаційних технологій для дорожньої безпеки тощо), яким в українському законодавстві не приділяється належної уваги; 5) аналіз нормативно-правових джерел Європейського Союзу дозволив дійти

висновку про пріоритетність у забезпеченні інформаційно-технічної безпеки саме Інтернет-безпеки; 6) на відміну від України, перед якою стоїть пріоритетне завдання щодо вдосконалення та розвитку інформаційної інфраструктури, для Європейського Союзу найактуальнішим є подолання розшарування суспільства на інформаційно освічених та неосвічених громадян; 7) враховуючи, що в основі регулювання прав та свобод громадян покладено міжнародно-правові акти, найбільш нормативно узгодженою складовою інформаційної безпеки між Україною та ЄС є інформаційна безпека у сфері прав та свобод [8, с.112].

Висновки і перспективи подальших досліджень.

Як висновок зазначимо, що інформаційна безпека Європейського Союзу охоплює такі аспекти:

- безпека використання Інтернету (“Safer Internet plus (2005 – 2008)”, “Safer Internet (1999 – 2005)”);
- безпека мережі (атаки на інформаційні системи, боротьба з кіберзлочинами);
- захист персональних даних.

Поряд з цим, зауважимо, що відсутність єдиної нормативної дефініції “інформаційна безпека ЄС”, зумовлює неоднозначне трактування її змісту, що ускладнює узгодження правових норм у сфері забезпечення інформаційної безпеки.

Використана література

1. Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки : Резолюція ООН від 1 грудня 1999 року. – Режим доступу : //www.un.org
2. Resolution adopted by the General Assembly UN [on the report of the First Committee (A/53/576)] “Development in the field of information abd telecommunication in the context of information security”. – Distr. General A/RES/53/70, 4 January, 1999, N.Y.
3. Макаренко Є.А. Міжнародна інформаційна політика: структура, тенденції, перспективи: дис... д-ра. політич. Наук : 23.00.04 / Націон. ун-т ім. Т.Шевченка. – К., 2003. – 475 с.
4. Convention on Cybercrime. Explanatory Report. Budapest, 23, November, 2001. Council of Europe. – Режим доступу : //www.europa.eu
5. Про атаки на інформаційні системи : Рішення Європейського Союзу від 24 лютого 2005 року. – Режим доступу : //www.europa.eu
6. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади : дис… д-ра. юрид. наук : 12.00.07 / Націон. ін-т внутр. справ. – Х., 2002. – 408 с.
7. Europe and Global Information Society. Recommendations of the High-Level Group on the Information Society to the Corfu European Council (Bangemann Group). European Commission, 1994.
8. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис… канд.-та. юрид. наук : 12.00.01 / Київський Націон. ун-т внутр. справ. – К., 2007. – 186 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~