УДК 341.232:[343.346.8:004]:061.1ЄС
Войціховський Андрій Васильович –
кандидат юридичних наук, доцент,
професор кафедри конституційного і
міжнародного права факультету № 4,
Харківського національного
університету внутрішніх справ

Andriy V. Voytsikhovkyy –
candidate of juridical sciences, associate professor,
professor of constitutional and international law
department of the Faculty No. 4 of
Kharkiv National University of Internal Affairs
(27 Lev Landau Avenue, Kharkiv, Ukraine)

Кібербезпека як важлива складова системи захисту національної безпеки європейських країн

Стаття присвячена дослідженню правових і організаційних засад забезпечення кібернетичної безпеки ЄС у сучасних умовах розвитку інформаційного суспільства. Автор з'ясовує концептуальні підходи щодо забезпечення безпеки в європейському кіберпросторі і визначає перспективні напрямки удосконалення існуючого механізму забезпечення кібербезпеки в ЄС.
Ключові слова: *Європейський Союз, кібербезпека, кіберзагроза, мережева і інформаційна безпека, інформаційна інфраструктура.*

Статья посвящена исследованию правовых и организационных основ обеспечения кибернетической безопасности ЕС в современных условиях развития информационного общества. Автор выясняет концептуальные подходы по обеспечению безопасности в европейском киберпространстве и определяет перспективные направления совершенствования существующего механизма обеспечения кибербезопасности в ЕС.
Ключевые слова: *Европейский Союз, кибербезопасность, киберугроза, сетевая и информационная безопасность, информационная инфраструктура.*

A.V. Voytsikhovkyy Cyber Security as an Important Component for the Ensuring the National Security of European Countries

The paper researches the issue on design and implementation of the EU policy on ensuring security in the European cyber space. These measures are related first of all to the development and improvement of legislation as well as creation of special structural divisions which regulate and are responsible for ensuring security in cyber space. Nowadays, ensuring cyber security is one of the strategical tasks of the European Union because majority of political and military conflicts exist in cyber space.

Researching the tendencies of the EU policy on ensuring cyber security the author discloses legal and organizational principles of cyber security of the EU in modern conditions of informational society, finds out conceptual approaches to ensuring security in European cyber space and identifies the future directions for improvement of the existing mechanism for ensuring cyber security in the EU.

Attention has been focused that accumulation of the big amount of information and its operation, provision of online services and recent connection of more than billion devices to electronic systems in the EU has not only advantages but a negative impact because cyber threats increase and spread. Understanding the essence of threats and taking into account the existing situation the paper presents a new vision of European cyber security and its legal regulation by the European Commission.

It has been stressed that strengthening of cyber stability in the EU is possible through international cooperation by creating and supporting reliable partner relations with the third countries to prevent and control

of cyberattacks. Moreover, the European Commission realizes that effective ensuring of security in European cyber space also depends on the development of cooperation between the states within the European police office (Europol), which activity, among others, is aimed at counteracting cybercrimes.

It has been concluded that research of normative and organizational principles of ensuring cyber security in the EU is of primary importance and its scientific presentation contributes to understanding of various transformations in network and information sphere. Under these circumstances it is relevant to do a complex research on European approach to the issue of ensuring cyber security, taking into account ambitions of Ukraine to the European integration.

Keywords: *European Union, cyber security, cyber threats, network and information security, information infrastructure.*

Постановка проблеми. Розуміючи сучасний стан та актуальність проблем у сфері телекомунікацій, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами, більшість країн світу проводять комплексні заходи щодо забезпечення національної кібербезпеки. Ці заходи пов'язані, перш за все, з розробкою та вдосконаленням нормативно-правових актів, а також створенням відомчих та державних структур, що регулюють і відповідають за забезпечення безпеки в кібернетичному просторі. Проблема забезпечення кібербезпеки є доволі важливим та складним питанням, а зневажливе ставлення держави до цього питання може призвести до непередбачуваних наслідків.

Активну політику в сфері кібербезпеки проводить й 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. Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки залишаються одним із стратегічних завдань діяльності ЄС, оскільки більшість політичних і військових конфліктів у світі відбуваються або віддзеркалюються саме у віртуальному просторі.

Дослідження питань нормативних і організаційних засад забезпечення кібербезпеки ЄС набуває виняткового сенсу, а його наукове висвітлення забезпечує розуміння сукупності перетворень, які відбуваються в мережевій і інформаційній сфері. За цих умов актуальним є комплексне дослідження європейського підходу до питання забезпечення кібербезпеки, особливо зважаючи на євроінтеграційні прагнення України.

Аналіз останніх досліджень і публікацій. Вивчення стану наукової розробленості проблем забезпечення кібербезпеки ЄС показало, що на сучасному етапі спеціального дослідження з цих питань не проводилося. Проте, окремі аспекти такої діяльності ЄС, розглядалися в наукових роботах І.М. Забара, О.Ю. Запорожець, В.К. Конах, В.А. Ліпкан, А.М. Орлеан, Є.Б. Тіхомірової та ін.

Невирішені раніше проблеми. Незважаючи на наявність великої кількості досліджень у цій сфері, динамічний характер розвитку інфраструктури в мережевій і інформаційній сфері, а також поширення кіберзлочинності вимагає нових наукових розробок й напрацювань щодо вироблення спільних підходів у протидії кіберзагрозам та інших заходів у сфері забезпечення кібербезпеки.

Метою даної статті є визначення концептуальних підходів щодо забезпечення безпеки в європейському кіберпросторі, дослідження сучасних правових і організаційних засад кібербезпеки ЄС, з'ясування перспективних напрямків удосконалення механізму забезпечення кібербезпеки в ЄС.

Виклад основного матеріалу. В 2001 р. 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. 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]

Європейське співтовариство відмічає, що мережева та інформаційна безпека вже стає ключовим фактором у розвитку інформаційного суспільства. Перш за все, мережі та інформаційні системи містять конфіденційні дані та економічно цінну інформацію, що підвищує стимул для атак. Атаки на інформаційні системи можуть мати серйозні у національному масштабі наслідки, як то збої у роботі систем комунікацій, витік конфіденційної інформації тощо.

10 березня 2004 р. було створено Європейське агентство з питань мережевої та інформаційної безпеки (European Union Agency for Network and Information Security - ENISA). ENISA – єдине з агентств ЄС, якому було визначено конкретний термін завершення її дії – 2020 р. Агентство функціонує з 1 вересня 2005 р., знаходиться в Іракліон, Крит, (Греція).

Місією ENISA є вдосконалення мережевої та інформаційної безпеки в Європейському Союзі. Агентство сприяє розвитку культури мережевої та інформаційної безпеки на користь громадян, споживачів, підприємств та громадських організацій ЄС, сприяючи безперебійному функціонуванню внутрішнього ринку ЄС.

ENISA допомагає Європейській комісії, державам-членам ЄС та приватному сектору виконувати вимоги мережевої та інформаційної безпеки, включаючи чинне та майбутнє законодавство ЄС. ENISA виступає центром експертизи як для держав-членів, так й для інституцій ЄС з отримання консультацій з питань, пов'язаних із мережевою та інформаційною безпекою. [2]

Європейське агентство з питань мережевої та інформаційної безпеки тісно співпрацює з Європейським поліцейським офісом (Europol) та Європейським центром боротьби з кіберзлочинністю (European Cyber Crime Centre), а також співпрацює з іншими установами ЄС, зокрема:

- Європейським агентством з питань правоохоронної підготовки (European Union Agency for Law Enforcement Training, CEPOL);
- Органом європейських регуляторів електронних комунікацій (Body of the European Regulators of Electronic Communications, BEREC);
- Європейським агентством оперативного управління великомасштабними IT-системами у сферах свободи, безпеки та юстиції (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, eu-LISA);
- Європейським агентством з авіаційної безпеки (European Aviation Safety Agency, EASA).

ENISA управляє загальноєвропейською програмою «Cyber Europe». Це - серія навчань з кіберінцидентів та управління кризовими ситуаціями на рівні ЄС для державного і приватного секторів країн-членів.

Вправи «Cyber Europe» – це симуляція великомасштабних інцидентів, пов'язаних з кібербезпекою, які, посилюючись, можуть стати кіберкризами. Вправи пропонують можливості для аналізу передових технічних заходів з кібербезпеки, вирішення проблем, пов'язаних із кризовими ситуаціями. Вправи «Cyber Europe» представляють собою сценарії, насичені реальними подіями, розробленими європейськими експертами з кібербезпеки. Кожна з вправ надає навчальний досвід для учасників. [3]

У своїй діяльності Агентство ENISA спирається на щорічні робочі плани/програми, які містять перелік основних пріоритетів і цілей та запланованих заходів для виконання поставлених завдань. У робочих програмах Агентства визначаються такі стратегічні пріоритети:

- підвищення здатності європейських електронних мереж протистояти зовнішнім впливам;
- розвиток співробітництва між країнами-членами ЄС у сфері мережевої та інформаційної безпеки;
- ідентифікація нових ризиків у сфері інформаційної безпеки і формування взаємної довіри.

З метою покращення співробітництва між судовими та іншими уповноваженими органами влади, включаючи поліцію та інші спеціалізовані правоохоронні органи держав-членів ЄС у сфері захисту інформаційних систем 24 лютого 2005 р. було прийняте Рамкове рішення Ради ЄС

2005/222/JHA щодо нападу на інформаційні системи, яка встановила мінімальні правила щодо визначення кримінальних злочинів та санкцій у сфері нападів на інформаційні системи.

У документі зазначається, що порушення захисту інформаційних систем є очевидними, зокрема в результаті загрози зі сторони організованої злочинності, і збільшення стурбованості щодо можливості терористичних спроб порушення інформаційних систем, які є частиною інфраструктури, що потребує особливого захисту держав-членів. Мають бути передбачені заходи, з метою співробітництва між державами-членами, для забезпечення ефективних дій спрямованих проти спроб порушення захисту інформаційних систем. Таким чином держави-члени повинні використовувати існуючу мережу діючих контактних пунктів зазначених у Рекомендації Ради ЄС 2001/С 187/02 щодо пунктів з цілодобової підтримки служби боротьби зі злочинами у сфері високих технологій від 25 червня 2001 р., забезпечуючи цілодобову підтримку в боротьбі з високотехнологічними злочинами та для обміну інформацією. Рамкове рішення передбачає, що умисний незаконний доступ до комп'ютерних систем, включаючи дані, що зберігаються в них, повинен бути покараний як кримінальний злочин. [4]

У травні 2007 р. Європейською комісією 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 напрямки політики ЄС у протидії кіберзлочинності. [5]

Згідно з документом, кіберзлочинність - це кримінальні дії, скоєні з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем. Це поняття включає три категорії злочинів:

- традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах);

- публікація протизаконного контенту в електронних медіа (дитяча порнографія, матеріали із закликами до расової ненависті і т.п.);

- специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо).

Важливо відмітити, що політика Європейської комісії в сфері протидії кіберзлочинності реалізується за наступними основними напрямами:

- участь у нормотворчому процесі (розробка і ухвалення міжнародно-правових документів у сфері протидії кіберзлочинності);

- заохочення міжнародного співробітництва правоохоронних органів країн-членів ЄС (організація науково-практичних конференцій, семінарів, тренінгів з питань протидії кіберзлочинності, створення цілодобових контактних пунктів у країнах-членах ЄС, розвиток платформи для навчання експертів у сфері протидії кіберзлочинністю та ін.);

- розвиток співробітництва між державним і приватним секторами у сфері протидії кіберзлочинності, зокрема, співпраця між правоохоронними органами та приватними компаніями;

- заохочення підписання країнами-членами ЄС та іншими країнами Конвенції про кіберзлочинність 2001 р. та ін. [6, с.39]

У березні 2009 р. було опубліковано Повідомлення Європейської комісії «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), 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. [7].

Згідно з цим документом, 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.

7 лютого 2013 р. Європейською комісією була схвалена Стратегія кібербезпеки «Відкритий, надійний та безпечний кіберпростір» (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace). Цей документ представляє собою всеосяжне бачення ЄС стосовно того, як краще запобігати та ліквідувати кіберзагрози.

У Стратегії відмічається, що інциденти, пов'язані з кібербезпекою, зростають все частіше, стають все більш складними і не знають кордонів. Ці інциденти можуть завдати серйозної шкоди безпеці та економіці держав. Для запобігання і знешкодження кіберзагроз рекомендується розвивати міждержавне співробітництво в цій сфері.

У документі також зазначається, що попередні зусилля Європейської комісії та окремих держав-членів ЄС були надто фрагментовані, щоб вирішити проблеми щодо забезпечення кібербезпеки. Саме Стратегія кібербезпеки сприятиме подальшим європейським цінностям свободи та демократії, спонукатиме безпечному зростанню цифрової економіки. Передбачені в документі конкретні заходи спрямовані на посилення кіберстійкості інформаційних систем, зменшенні кіберзлочинів та зміцненні міжнародної політики ЄС щодо кібербезпеки та кібероборони.

Стратегія формулює бачення ЄС щодо кібербезпеки з п'яти пріоритетів:

1. Досягнення кіберстійкості.

2. Суттєве скорочення кіберзлочинності.

3. Розробка політики кібероборони, пов’язаної зі Спільною політикою безпеки і оборони.

4. Розвиток виробничих і технологічних ресурсів для кібербезпеки.

5. Створення узгодженої міжнародної політики кіберпростору для ЄС і просування основних цінностей ЄС.

У Стратегії зауважується, що «міжнародна політика в сфері кіберпростору в ЄС сприяє повазі основних цінностей ЄС, визначає норми відповідальної поведінки, виступає за застосування існуючих міжнародних документів щодо кіберпростору, а також допомагає країнам, що не є членами ЄС, розвивати спроможність у сфері кібербезпеки, а також сприяти міжнародному співробітництву в протидії кіберзлочинності». [8]

Одразу після оприлюднення Стратегії кібербезпеки було розпочато роботу над відповідною директивою. Важливо наголосити, що цей документ розроблявся не окремо від інших напрямків, а в якості частини Стратегії Єдиного Цифрового Ринку (Digital Single Market Strategy), з одного боку, і частини Європейського Порядку денного з питань безпеки (European Agenda on Security), з іншого. [9]

Стратегія та Порядок денний були оприлюднені навесні 2015 р., в липні 2016 р. Європейська комісія презентувала «Додаткові заходи по сприянню розвитку індустрії кіберзахисту», а 6 липня 2016 р. була ухвалена Директива ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (Concerning measures for a high common level of security of network and information systems across the Union - NIS Directive). [10]

Ця Директива закладає єдині правила та вимоги в сфері кібербезпеки для всіх країн ЄС, але залишає за кожною країною-членом право вжити власних заходів щодо імплементації норм цієї Директиви в національне законодавство.

Для досягнення мети Директиви (забезпечення більш високого рівня мережевої та інформаційної безпеки в межах ЄС) необхідно вжити заходів в трьох основних напрямках:

- підвищити спроможність системи кібербезпеки на національному рівні;

- підвищити рівень європейського співробітництва;

- запровадити управління ризиками та зобов’язати сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових послуг.

Для підвищення спроможності кібербезпеки на національному рівні держави-члени ЄС повинні розробити національну стратегію мережевої та інформаційної безпеки (яка повинна включати в себе стратегічні цілі, пріоритети та державне підґрунтя, заходи з

підготовки до кіберінцидентів, реагування на них та відновлення після них, засади державно-приватного партнерства, програму освітніх, тренувальних заходів та заходів з підвищення обізнаності, план науково-дослідницьких робіт, план оцінки та управління ризиками, список стейкголдерів, відповідальних за реалізацію стратегії), визначити один чи більше державних органів, що будуть відповідати за виконання Директиви, створити одну чи більше команд реагування на комп'ютерні надзвичайні події.

Серед основних загроз національним кіберпросторам розроблені національні стратегії країн-членів ЄС визначають:

- Кібершпигунство та військові дії, які здійснюються за підтримки або з відома держави. Всі технологічно розвинені держави та корпорації стають об'єктом кібершпигнуства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією.

- Використання Інтернету у терористичних цілях. Терористичні угрупування використовують Інтернет з метою пропаганди, збору коштів і вербування прихильників.

- Кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе програмне забезпечення.

Відповідно, національне законодавства країн, як правило, регулюють питання:

- захисту персональних даних (Нідерланди, Естонія, Швеція, Фінляндія, Іспанія);

- захисту електронної комерції та безпеки електронних транзакцій та платіжних інструментів (Польща, Естонія, Італія);

- захисту важливих об'єктів інфраструктури та інформаційних систем (Франція). [11, с.3]

13 вересня 2017 р. Європейська комісія представила документ «Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС» (Resilience, Deterrence and Defence: Building strong cybersecurity for the EU), в якому зазначено, що кібербезпека має вирішальне значення для процвітання та безпеки країн-членів. Якщо не приймати заходи по забезпеченню кібербезпеки, то ризик загроз збільшуватиметься відповідно до цифрових перетворень. Ризик політично-мотивованих нападів на цивільні цілі та недоліки військового кіберзахисту ще більше поглиблює ризик. Хоча країни-члени залишаються відповідальними за національну безпеку, масштаби та транскордонний характер кіберзагроз створюють стимули для держав-членів щодо розробки та підтримки більш потужних національних можливостей для забезпечення кібербезпеки ЄС в цілому. Сильна кіберстійкість вимагає колективного та широкомасштабного підходу. Це вимагає більш надійних та ефективних структур для сприяння кібербезпеки та реагування на кібератаки в країнах-членах, а також в установах та органах ЄС. [12]

Європейська комісія наголошує на тім, що повна імплементація всіма країнами-членами Директиви NIS дозволить покращити стійкість за рахунок вдосконалення можливостей національної кібербезпеки; сприяти кращому співробітництву між державами-членами; і вимагати від приватного сектора приймати ефективні заходи з управління ризиками та повідомляти про серйозні інциденти національним органам влади.

З метою підвищення рівня європейського співробітництва створюються спеціальні мережі та Група співробітництва, яка буде забезпечувати планування, керування, обмін інформацією та підготовку звітів щодо стану кібербезпеки в країнах-членах ЄС.

Найбільш важливі законодавчі новели стосуються умов роботи операторів базових послуг та провайдерів цифрових послуг. Визначення «операторів базових послуг» кожна країна дає сама, але на підставі спільних для усього ЄС критеріїв:

- підприємство (незалежно від форми власності) надає послугу, яка є базовою для підтримки критичної соціально-економічної діяльності;

- надання такої послуги потребує використання мережевих або інформаційних систем;

- порушення безпеки буде мати значний руйнівний вплив на надання базової послуги.

В першу чергу це стосується наступних секторів:

- енергетика: електроенергія, нафта, газ;

- транспорт: повітряний, залізничний, водний, автодорожній;
- банки, кредитні установи;
- інфраструктура фінансового ринку: біржі, центральні контрагенти;
- заклади охорони здоров'я;
- постачання питної води;
- цифрова інфраструктура: точки обміну Інтернет-трафіком, провайдери системи доменних імен, сервіс-провайдери, реєстратури доменних імен верхнього рівня.

Під провайдерами цифрових послуг, які підпадають під дію цієї Директиви, маються на увазі онлайнові торгівельні майданчики, постачальники хмарних послуг, пошукові системи.

Такі підприємства мають вжити необхідних (технічних та організаційних) заходів для того, аби попередити ризики кіберінцидентів, забезпечити мережеву та інформаційну безпеку (у відповідності до потенційних ризиків), належним чином відреагувати на кіберінциденти з метою мінімізації шкоди, повідомити компетентні органи про кіберінциденти. Директивою також передбачається дотримання міжнародних стандартів цими підприємствами, постійне проведення моніторингу, аудиту та тестування.

Вірогідним фактом є те, що накопичення великих масивів інформації і оперування ними, надання електронних послуг, і початкове підключення в Європейському Союзі, у найближчі роки, більше мільярда пристроїв до електронних мереж надає не лише переваги, але й здійснює негативний вплив - зростає кількість, обсяг, розмах і різноманітність кібернетичних загроз. Розуміючи суть загроз і враховуючи існуючу ситуацію, Європейська комісія у 2017 р. запропонувала своє бачення нової, викликаної часом, архітектури європейської кібернетичної безпеки та її правове забезпечення.

Задля реалізації цієї мети Європейська комісія запропонувала нові інструменти, включаючи створення Європейського агентства з кібербезпеки і Європейського центра досліджень та компетенції з кібербезпеки, щоб допомогти країнам-членам захиститися від таких кібернападів.

Європейське агентство з кібербезпеки створять на основі існуючого Європейського агентства з питань мережевої та інформаційної безпеки (ENISA). Воно матиме постійний мандат та можливість надавати країнам-членам ефективну допомогу та реагувати на кібератаки. Це покращить готовність ЄС реагувати на кіберзагрози, організовуючи щорічні загальноєвропейські вправи з кібербезпеки та забезпечуючи кращий обмін інформацією про загрозу та знання шляхом створення центрів обміну інформацією та аналізу.

Європейське агентство з кібербезпеки допомагатиме запровадити та впровадити загальноєвропейську систему сертифікації. Нові європейські сертифікати з кібербезпеки забезпечать надійність мільярдів пристроїв, які мають відношення до сьогоднішньої критичної інфраструктури, такої як енергетичні та транспортні мережі. Сертифікати з кібербезпеки будуть визнані країнами-членами, таким чином, знизяться адміністративні витрати та витрати для компаній.

На думку Європейської комісії, протидія кіберзагрозам потребує з боку ЄС масштабних інвестицій у технології кібербезпеки, продукти, процеси та експертизу для досягнення технологічної автономії кібербезпеки та захисту своєї цифрової економіки, суспільства та демократії. Ці можливості є також важливими для сприяння глобальним зусиллям, спрямованим на створення безпечного кіберпростору для всіх. На основі роботи країн-членів та державно-приватного партнерства Європейська комісія пропонує створення мережі з кібербезпеки з *Європейським центром досліджень та компетенції з кібербезпеки*. Даний Центр допоможе розробити та впровадити інструменти та технології, необхідні для усунення постійно змінюваних кіберзагроз. Він буде доповнювати зусилля з нарощування потенціалу в цій сфері на рівні ЄС та на національному рівні. [13]

Разом з цим, Європейська комісія пропонує додатково посилити кіберзахист шляхом прийняття нової Директиви з боротьби з шахрайством та підробкою безготівкових засобів платежу. Відповідно до Стратегії кібербезпеки ЄС, а також Стратегії єдиного цифрового ринку, нова Директива посилить здатність країн-членів проводити кримінальне переслідування за шахрайство з безготівковими платежами.

Зміцнення глобальної кібернетичної стабільності Європейський Союз вбачає через

міжнародне співробітництво шляхом створення та підтримки надійних партнерських відносин з третіми країнами задля запобігання та стримування кібератак. ЄС вже співпрацює з США, Японією, Індією, Південною Кореєю та Китаєм. Також діють тісні консультації з міжнародними організаціями, такими як Організація Північноатлантичного договору (НАТО), Асоціація держав Південно-Східної Азії (АСЕАН), Організація з безпеки і співробітництва в Європі (ОБСЄ), Рада Європи (РЄ) та Організація економічного співробітництва і розвитку (ОЕСР) та ін. [14, с.9-10]

Європейська комісія усвідомлює той факт, що ефективність забезпечення безпеки в європейському кіберпросторі також залежить від розвитку співпраці держав у рамках міжнародних органів, діяльність яких направлена на протидію кіберзлочинності. З цією метою у 2013 р. в Європолі (Європейському поліцейському офісі) був створений *Європейський центр боротьби з кіберзлочинністю* (European CyberCrime Centre), який розпочав свою роботу з січня 2013 р. в м. Гаага (Нідерланди). Щоб збільшити ймовірність притягнення злочинців до відповідальності, Європейська комісія наполягає терміново покращити ситуацію щодо виявлення кіберзлочинців шляхом посилення Європейського центру боротьби з кіберзлочинністю новими кадрами - кіберекспертами.

Серед пріоритетів Центру – розслідування шахрайства через онлайн-мережі, зокрема у системі електронного банкінгу та інших видів фінансової діяльності, протидія сексуальній експлуатації дітей через мережу Інтернет, а також розслідування інших злочинів, що посягають на безпеку критично важливої інфраструктури та інформаційних систем ЄС. Працівники цієї структури займаються підвищенням кваліфікації слідчих та прокурорів країн-членів ЄС та застерігають громадськість від нових кіберзлочинів. [15]

Щороку Європейський центр боротьби з кіберзлочинністю публікує звіт про кіберзагрози організованої злочинності (IOCTA). Звіт є головним стратегічним документом про основні висновки, нові загрози та події щодо кіберзлочинності. IOCTA надає основні рекомендації правоохоронним органам, державним органам, щоб вони могли ефективно та узгоджено реагувати на кіберзлочинність. [16]

Європейський центр боротьби з кіберзлочинністю не ставить собі за мету конкурувати з поліцейськими службами країн-членів ЄС. Центр позиціонує себе як платформа для співробітництва правоохоронних органів країн-членів ЄС. Проте й інші зацікавлені країни, які вже зараз співпрацюють з ЄС у цій сфері, зможуть скористатися напрацюваннями Центру. [15] Нагадаємо, що Україна 14 грудня 2016 р. підписала Угоду між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво. [17]

Основними способами підвищення компетентності в сфері кібербезпеки визначено організацію навчань (тренінгів) з питань кібербезпеки та проведення досліджень. Сюди відноситься, зокрема, встановлення вимог до знань в сфері інформаційної безпеки та кіберзахисту для робітників державного і приватного секторів та впровадження відповідної системи оцінювання, підвищення рівня підготовленості до кризових ситуацій в державному та приватному секторах, а також створення в Естонії під егідою НАТО Центру експертизи з питань кооперативної кібероборони - CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence).

Діяльність Центру CCDCOE направлена на співпрацю та обмін інформацією в НАТО, а також серед країн-членів та країн-партнерів НАТО з питань кібер-оборони шляхом навчання, наукових досліджень та розвитку, узагальнення отриманих практичних «уроків» та проведення консультацій. [18]

Діяльність щодо правового регулювання сфери кібербезпеки включає також 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; започаткування ініціатив у законотворчій діяльності на міжнародному рівні тощо.

Діяльність щодо зміцнення міжнародної співпраці з питань кібербезпеки передбачає винесення проблем кібербезпеки на міжнародний «порядок денний»; сприяння

ратифікації країнами Конвенції Ради Європи про кіберзлочинність 2001 р. (Україна ратифікувала 7 вересня 2005 р.); обговорення проблем кібербезпеки на міжнародних науково-практичних конференціях, семінарах та форумах; надання підтримки міжнародним корпораціям, асоціаціям, дослідницьким інститутам та неурядовим організаціям, які займаються проблемами кібербезпеки; просування кращої практики в сфері кібербезпеки на міжнародному рівні та ін.

Висновки. Проведений аналіз тенденцій у політиці ЄС щодо забезпечення кібернетичної безпеки, зважаючи на посилення кібербезпекової компоненти у системі національної безпеки країн-членів ЄС, дозволив зробити наступні висновки:

- Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз для національної безпеки європейських країн. Сучасні інформаційні технології, перетворюють інформаційні системи на надзвичайно вразливі для реалізації кібернетичних загроз об'єкти. В цих умовах, головним завданням європейських, та й інших країн світу є вжиття заходів, що дозволять принципово зменшити (а подекуди - унеможливити повністю) негативні наслідки від кібератак. Неабияку роль у виробленні єдиних підходів щодо забезпечення кібернетичної безпеки як складової національної безпеки європейських країн відіграє Європейський Союз.
- Європейський Союз активно модернізує власні сектори безпеки у кіберпросторі у відповідності до викликів сучасності. Цей процес відбувається шляхом: впорядкуванням нормативної бази, що має забезпечити цілісність державної політики в даній сфері; вироблення європейських керівних принципів щодо забезпечення стійкості і стабільності мережі Інтернет та їхнє просування на міжнародній арені; збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту; посилення контролю за національним інформаційним простором; зміцнення захисних механізмів для критичної інформаційної інфраструктури ЄС; проведення загальноєвропейських навчань та досліджень з проблем безпекових інцидентів в мережі Інтернет; посилення співпраці між державним і приватним секторами; створення європейського форуму для обміну інформацією між країнами-членами; створення європейської системи раннього сповіщення про кіберзагрози та ін.
- Зважаючи на значний прогрес і досвід Європейського Союзу у виробленні й удосконаленні механізму забезпечення кібербезпеки європейських країн, Україна повинна стати активним учасником цих безпекових процесів. З одного боку, враховуючи інтеграційні прагнення України, це буде сприяти поліпшенню іміджу держави, а з іншого – впливати на формування організаційно-правової основи забезпечення національної кібербезпеки України. В умовах розробки Україною національного законодавства у сфері кібернетичної безпеки дієвим може виступити врахування досвіду ЄС, перспективних майбутніх планів, програм і проектів, а також участь у спільних європейських проектах із забезпечення кібернетичної безпеки. В умовах гібридної війни та запровадження практик електронного врядування питання кібернетичної безпеки для України повинні бути в центрі уваги державної політики.
- Посилення кіберскладової у системах державної безпеки ЄС обумовлює необхідність якнайшвидшого впорядкування політики Української держави у сфері забезпечення кібербезпеки. Ключовим в цьому процесі має стати визначення цілей та методів їх досягнення (в першу чергу коротко- та середньострокових).

Правильно розроблена стратегія зовнішньої політики України щодо співпраці з ЄС у сфері кібернетичної безпеки, безумовно, призведе взаємовигідного партнерства у вирішенні проблемних питань щодо забезпечення національних інтересів у сфері кібербезпеки.

Список використаних джерел:

1. Network and information security: proposal for a european policy approach: adopted by the European Commission on 6 June 2001 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298 (дата звернення 01.06.2018).

2. About ENISA / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa (дата звернення 01.06.2018).

3. Cyber Europe / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (дата звернення 01.06.2018).

4. Council framework decision 2005/222/JHA on attacks against information systems: adopted by the Council of the European Union on 24 February 2005 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222 (дата звернення 03.06.2018).

5. Towards a general policy on the fight against cyber crime: adopted by the European Commission on 22 May 2007 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560 (дата звернення 02.06.2018).

6. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки. *Актуальні проблеми міжнародних відносин.* 2009. Вип. 87, ч. II. С. 36-45.

7. Communication from the Commission on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience»: adopted by the European Commission on 30 March 2009 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149 (дата звернення 04.06.2018).

8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (дата звернення 03.06.2018).

9. EU cybersecurity initiatives working towards a more secure online environment / European Union. URL: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf (дата звернення 04.06.2018).

10. Concerning measures for a high common level of security of network and information systems across the Union - NIS Directive: Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 / Official Journal of the European Union. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення 05.06.2018).

11. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. Київ: Інфоцентр, Європейський інформаційно-дослідницький центр, Лабораторія законодавчих ініціатив, 2016. 37 с.

12. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU: adopted by the European Commission on 13 September 2017 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN (дата звернення 05.06.2018).

13. State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks: European Commission - Press release, 19 September 2017 / European Union. URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm (дата звернення 05.06.2018).

14. Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій. *Журнал європейського і порівняльного права*. 2017. Вип. 3. С. 2-13.

15. Гассельбах К., Завгородня І. Європейський центр боротьби з кіберзлочинністю починає роботу // DW. Made for minds. URL: http://p.dw.com/p/17HRW (дата звернення 06.06.2018).

16. Internet Organised Crime Threat Assessment (IOCTA) / Europol. lURL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment (дата звернення 06.06.2018).

17. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво: міжнародний договір від 14.12.2016 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/984_001-16/paran2#n2 (дата звернення: 05.06.2018).

18. Центр експертизи з питань кооперативної кібер -оборони (CCDCOE) / North Atlantic Treaty Organization. URL: https://www.nato.int/docu/other/ukr/pdf/CCD%20COE%20presentation%20ukr.pdf (дата звернення: 06.06.2018).

References:

1. Network and information security: proposal for a european policy approach: adopted by the European Commission on 6 June 2001 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298 (дата звернення 01.06.2018).

2. About ENISA / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa (дата звернення 01.06.2018).

3. Cyber Europe / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (дата звернення 01.06.2018).

4. Council framework decision 2005/222/JHA on attacks against information systems: adopted by the Council of the European Union on 24 February 2005 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222 (дата звернення 03.06.2018).

5. Towards a general policy on the fight against cyber crime: adopted by the European Commission on 22 May 2007 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560 (дата звернення 02.06.2018).

6. Zaporozhets O.Y. Politika Yevropeyskogo Soyuzy v sferi informatsiynoyi bezpeky. *Aktualni problemy mizhnarodnyh vidnosyn.* 2009. Vyp. 87, ch. II. Pp. 36-45.

7. Communication from the Commission on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience»: adopted by the European Commission on 30 March 2009 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149 (дата звернення 04.06.2018).

8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (дата звернення 03.06.2018).

9. EU cybersecurity initiatives working towards a more secure online environment / European Union. URL: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf (дата звернення 04.06.2018).

10. Concerning measures for a high common level of security of network and information systems across the Union - NIS Directive: Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 / Official Journal of the European Union. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення 05.06.2018).

11. Zakonodavstvo ta strategiyi y sferi kiberbezpeky krayin Yevropeyskogo Soyuzu, SSHA, Kanady та inshyh. Informatsiyina dovidka, pidgotovlena Yevropeyskym informatsiyino-doslidnytskym tsentrom na zapyt narodnogo deputata Ukrayiny. Kyyiv: Infotsentr, Yevropeyskyy informatsiyno-doslidnytskyy tsentr, Laboratoriya zakonodavchyh initsiatyvs, 2016. 37 p.

12. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU: adopted by the European Commission on 13 September 2017 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN (дата звернення 05.06.2018).

13. State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks: European Commission - Press release, 19 September 2017 / European Union. URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm (дата звернення 05.06.2018).

14. Zabara I.M. Formuvannya suchasnyh pravovyh zasad kibernetychnoyi bezpeky Yevropeyskogo Soyuzu v ymovah poshyrennya novyh innovatsiynyh tehnologiy. *Zhurnal yevropeyskogo i porivnyalnogo prava*. 2017. Vyp. 3. Pp. 2-13.

15. Gasselbah K., Zavgorodnya I. Yevropeyskyy tsentr borotby z kiberzlochynnistyu pochynaye robotu // DW. Made for minds. URL: http://p.dw.com/p/17HRW (дата звернення 06.06.2018).

16. Internet Organised Crime Threat Assessment (IOCTA) / Europol. lURL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment (дата звернення 06.06.2018).

17. Ugoda mizh Ukrayinoyu ta Yevropeyskym politseyskym ofisom pro operatyvne ta strategichne spivrobitnytstvo: mizhnarodnyy dogovir vid 14.12.2016 // Baza dannyh «Zakonodavstvo Ukrayiny» / Verhovna Rada Ukrayiny. URL: http://zakon3.rada.gov.ua/laws/show/984_001-16/paran2#n2 (дата звернення: 05.06.2018).

18. Tsentr ekspertyzy z pytan kooperatyvnoyi kiber-oborony (CCDCOE) / North Atlantic Treaty Organization. URL: https://www.nato.int/docu/other/ukr/pdf/CCD%20COE%20presentation%20ukr.pdf (дата звернення: 06.06.2018).