

## *International experience in the field of ensuring information security of person, society, state*

---

УДК 007:004.56:341.174(4)

*БОЙКО Віктор Дмитрович  
ВАСИЛЕНКО Микола Дмитрович  
КУХАРЕНКО Сергій Вікторович*

### **КІБЕРБЕЗПЕКА В ЄС ТА КРАЇНАХ-ЧЛЕНАХ: ГЕНЕЗИС ТА ПРОБЛЕМИ ЇЇ ПІДВИЩЕННЯ**

**Постановка проблеми.** На теперішній час у багатьох чільних країнах світу вже сформовані загальнодержавні мережі кібернетичної безпеки, які здатні досить швидко акумулювати сили та засоби державних органів і приватного сектору для протидії кіберзагрозам, тим самим забезпечуючи кібербезпеку своїх країн. Це певною мірою стосується ЄС та його країн-членів.

**Аналіз останніх досліджень і публікацій.** Сьогодні існує чимало праць з питань кібербезпеки, в тому числі й питань кібербезпеки в ЄС. Однак статей, присвячених дослідженням з позицій системного підходу щодо генезису розвитку кібербезпеки в цих утвореннях в контексті підвищення якості самої кібербезпеки, небагато. Автори звертають увагу на роботи, де обговорюються проблеми якості безпеки інформаційно-комунікаційних систем [1; 2]. В роботах соціогуманітарного напрямку інших авторів (А. В. Войціховський, С. В. Демедюк, І. М. Забара, О. Ю. Запорожець, В. К. Конах, В. А. Ліпкан, Р. В. Лук'янчук, А. М. Орлеан, Є. Б. Тіхомірова та ін.) вивчалися в основному питання законодавчого характеру в ЄС або в окремих країнах у конкретні часові періоди.

**Метою статті** є дослідження генезису кібербезпеки в ЄС та країнах-членах на законодавчому рівні і виявлення його можливих кореляцій та залежності від науково-технічного прогресу.

**Виклад основного матеріалу.** Проблеми кібербезпеки виникали разом зі становленням інформаційно-комунікаційних систем (ІКС). У зв'язку з цим вони неодноразово розглядалися на різних міжнародних та національних рівнях, постійно шукаючи рішень в контексті розвитку самих ІКС.

Передусім розвиток у сфері боротьби з міжнародною та національною кіберзлочинністю започаткувала Конвенція Ради Європи про кіберзлочинність (Будапешт, листопад 2001 р.). При цьому її було ратифіковано більше ніж півсотнею країн, а серед країн-учасників були й країни, що не є країнами-членами РЄ, як-от США, Канада, Японія, Мексика, Австралія та багато інших. Розглянемо більш детально її основні положення. Зауважимо, що положення Конвенції діють не у всіх країнах адже відомо, що чотири країни підписали, але не ратифікували її, та є противники підписання – Росія та Китай. Як зазначено у преамбулі, «Конвенція є необхідною для зупинення дій, спрямованих проти

## ***Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави***

конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це прописано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва». При цьому особлива увага звертається на потреби досягнення паритету правоохоронних інтересів і пошани до фундаментальних прав людини таких, як право кожного безперешкодно дотримуватись поглядів, право на свободу слова, включаючи право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на кордони, права на повагу до приватного життя, а також права на захист особистої інформації.

Конвенція передбачає впровадження кримінальної відповідальності на національному рівні за такі групи злочинів:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями);

- комп'ютерні правопорушення (підробка та шахрайство із застосуванням комп'ютерів);

- правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією);

- правопорушення віднесені до порушення авторських та суміжних прав.

Невдовзі Генеральна Асамблея (ГА) ООН прийняла Резолюцію, зміст якої був пов'язаний саме з питаннями забезпечення кібербезпеки [3]. Зокрема, у Резолюції йшлося про конкретні заходи: про необхідність створення системи глобальної культури кібербезпеки. ГА ООН пропонувала державам-членам відповідно віднестися до створення глобальної культури кібербезпеки, зокрема, в рамках їхніх зусиль щодо розвитку у своїх суспільствах культури кібербезпеки при застосуванні та використанні інформаційних технологій. В Резолюції відзначалося також важливе значення міжнародного співробітництва для досягнення кібербезпеки шляхом підтримки національних зусиль, спрямованих на укріплення людського потенціалу, розширення можливостей в плані навчання і зайнятості, покращення державних послуг і підвищення якості життя за рахунок використання передових, надійних та безпечних інформаційно-комунікаційних технологій (ІКТ) і мереж, а також сприяння забезпеченню загального доступу [3]. Це сприяло прийняттю в наступному році (2003 р.) Женевської декларації [4], в якій зазначалася необхідність прискорення впровадження глобальної культури кібербезпеки в співробітництві з усіма зацікавленими сторонами і компетентними міжнародними органами. Такі зусилля мали спиратися на широке

## *International experience in the field of ensuring information security of person, society, state*

міжнародне співробітництво. У рамках глобальної культури кібербезпеки вважалося доцільним підвищувати безпеку і забезпечувати захист даних і недоторканності приватного життя (п. 35). Практичною реалізацією Резолюції стало прийняття Туніської програми для інформаційного суспільства (п. 39), де наголошувалося таке: «Ми прагнемо підвищувати довіру і безпеку при використанні ІКТ шляхом зміцнення основи для довіри. Ми знову підтверджуємо необхідність далі просувати, розвивати і впроваджувати у співробітництві з усіма заінтересованими сторонами глобальну культуру кібербезпеки, як це викладено в резолюції 57/239 ГА ООН та інших відповідних регіональних основоположних документах. Ця культура потребує національних дій та активізації міжнародного співробітництва для зміцнення безпеки при підвищенні захисту особової інформації, недоторканності приватного життя і даних» [5]. В ЄС у зв'язку з розумінням важливості проблеми кібербезпеки в 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security), яке функціонує й по теперішній час, спершу надаючи настанови та рекомендації з інформаційної безпеки, а згодом розширило сферу своєї діяльності на вирішення питань кібербезпеки, виступаючи центром експертизи як для держав-членів, так й для інституцій ЄС з отримання консультацій з питань, пов'язаних із мережевою та інформаційною безпекою [6]. Завдяки цьому кроку у більшості країн-членів було створено національні стратегії

кібербезпеки та національні план із захисту інформаційної інфраструктури. Знаковою подією сталося ухвалення в рамках ЄС (2013 р.) Стратегії кібербезпеки, метою якої можна вважати відкритий, надійний і безпечний кіберпростір. Для цього передбачені заходи з наступних напрямків [7]:

- 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 його основних цінностей.

А пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, стали [8, с. 30]:

- а) свобода та відкритість: Стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;
- б) застосування законодавства ЄС у кіберпросторі у тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на усьому глобальному суспільстві: від пересічних громадян до держав;
- с) розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством.

Після оприлюднення Стратегії було розпочато роботу над відповідною директивою. Важливо наголосити, що цей документ розроблявся не окремо від інших напрямків, а як

## *Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави*

частина Стратегії єдиного цифрового ринку (Digital Single Market Strategy), з одного боку, і частина Європейського Порядку денного з питань безпеки (European Agenda on Security), з іншого [9].

Стратегія та Порядок денний були оприлюднені навесні 2015 року, в липні 2016 року Європейська Комісія презентувала «Додаткові заходи по сприянню розвитку індустрії кіберзахисту». Також у липні 2016 року була ухвалена Директива ЄС 2016/1148 щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (NIS Directive) [10]. Директива є значним кроком до збільшення кіберстійкості ЄС та створення спільної відповіді на кіберзагрози в ЄС, адже вона ґрунтується на формі мінімальної гармонізації, яка дозволяє визначити багато деталей окремими країнами-членами Європейського Союзу з супутнім ризиком меншого впливу [11]. Тож ця Директива закладає єдині правила та вимоги у сфері кібербезпеки для всіх країн ЄС, але залишає за кожною країною-членом право вжити власних заходів щодо імплементації норм цієї Директиви в національне законодавство.

Її метою стало досягнення високого загального рівня безпеки мережевих та інформаційних систем у рамках Союзу. Так, для досягнення цієї мети Директива зобов'язала країни-члени: ухвалити відповідні національні стратегії; створювати групи зі співробітництва з метою підтримки і сприяння стратегічній співпраці та обміну інформацією між державами-членами; створювати групи реагування на

комп'ютерні інциденти з метою розвитку довіри між державами-членами та швидкого й ефективного оперативного співробітництва; встановлювати вимоги безпеки для операторів цифрових послуг тощо.

Для досягнення мети Директиви були вжиті заходи в трьох основних напрямках:

- підвищити спроможність системи кібербезпеки на національному рівні;
- підвищити рівень панєвропейського співробітництва;
- запровадити управління ризиками та зобов'язати сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових послуг.

Для підвищення спроможності кібербезпеки на національному рівні країни-члени ЄС мали розробити національну стратегію мережевої та інформаційної безпеки (яка має 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 стейкхолдерів, відповідальних за реалізацію стратегії), визначити один чи більше державних органів, що будуть відповідати за виконання Директиви, створити одну або більше команд реагування на комп'ютерні надзвичайні події (команда комп'ютерної безпеки з реагування на інциденти) CSIRT (Computer Security Incident Team).

## *International experience in the field of ensuring information security of person, society, state*

---

CSIRT відповідають за:

- моніторинг та реагування на випадки кіберзагроз;
- надання аналізу ризиків та аналізу інцидентів та ситуаційної обізнаності;
- участь у мережі CSIRT;
- співпраця з приватним сектором;
- сприяння використанню стандартизованої практики для інцидентів та класифікації ризиків та інформації.

Для підвищення рівня панєвропейського співробітництва створюються спеціальні мережі та група співробітництва, яка буде забезпечувати планування, керування, обмін інформацією та підготовку звітів щодо стану кібербезпеки в усіх країнах ЄС.

Завдання групи співробітництва включають: забезпечення керівництва мережею CSIRT; обмін найкращими практиками щодо ідентифікації постачальників основних послуг; надання допомоги країнам ЄС у розбудові можливостей кібербезпеки; обмін інформацією та найкращими практиками щодо підвищення обізнаності та навчання, досліджень і розробок; обмін інформацією та збір кращих практик щодо ризиків та інцидентів; обговорення способів оповіщення про інцидент.

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

1. Підприємство (незалежно від форми власності) надає послугу, яка є базовою для підтримки критичної соціально-економічної діяльності.

2. Надання такої послуги потребує використання мережевих або інформаційних систем.

3. Порушення безпеки буде мати значний руйнівний вплив на надання базової послуги.

В першу чергу, це стосується таких секторів, як енергетика (нафта, газ, електроенергія); транспорт (повітряний, залізничний, водний, автодорожний); банки (кредитні установи); інфраструктура фінансового ринку; 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 онлайн-нові торговельні майданчики, постачальники хмарних послуг, пошукові системи [10].

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.

Згодом (вересень 2017 р.) Європейська комісія оприлюднила оновлену редакцію Стратегії кібербезпеки. Вона була призначена для поліпшення

## *Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави*

---

захисту критично важливої інфраструктури Європи і підвищення цифрового самоствердження ЄС щодо інших регіонів світу. Однак реформована стратегія досі залишає відкритим низку питань щодо того, як її мета «відкритого, безпечного і надійного кіберпростору» буде надійно захищена як всередині, так і зовні. У ЄС немає ні належним чином певної стабільності або стримування, ні досить ясного пояснення того, як він має намір подолати інституційну фрагментацію і відсутність правових повноважень в питаннях кібербезпеки [12].

Пропозиція щодо регулювання Європейського Парламенту та Ради щодо ENISA («Агентства ЄС з кібербезпеки») і скасування Регламенту (ЄС) 526/2013 та щодо сертифікації кібербезпеки інформаційних та комунікаційних технологій («Закон про кібербезпеку»). Його основними положеннями є призначення ENISA як постійного агентства ЄС з кібербезпеки та структури для створення європейських схем сертифікації кібербезпеки з метою забезпечення адекватного рівня кібербезпеки продуктів і послуг ІКТ в ЄС [13]. При цьому згідно зі статтею 43 «Закону про кібербезпеку» європейська схема сертифікації кібербезпеки повинна свідчити про те, що продукти і послуги ІКТ, які були сертифіковані відповідно до такої схеми, відповідають зазначеним вимогам щодо їх здатності протистояти з певним рівнем впевненості діям, спрямованим на компрометацію доступності, достовірності, цілісності або конфіденційності збережених або переданих або оброблених даних або функцій чи послуг, пропонованих або доступних

через ці продукти, процеси, послуги та системи [13]. Елементами європейської схеми сертифікації кібербезпеки стали: предмет і обсяг сертифікації, включаючи тип або категорії охоплених продуктів і послуг ІКТ; детальна специфікація вимог кібербезпеки, щодо яких оцінюються конкретні продукти та послуги ІКТ, наприклад, посиленням на стандарти ЄС або міжнародні стандарти, або технічні специфікації; де це можливо, один або більше рівнів гарантування, де схема передбачає використання міток або ярликів, умови, при яких такі знаки або ярлики можуть використовуватися; там, де спостереження є частиною схеми, застосовуються правила моніторингу відповідності вимогам сертифікатів, включаючи механізми для демонстрації постійної відповідності зазначеним вимогам кібербезпеки; умови надання, збереження, продовження, розширення та скорочення обсягів сертифікації та інші (див. ст. 47 [13]). Крім того, відповідно до ст. 46 існує три види гарантії європейської схеми сертифікації кібербезпеки: базовий, значний та/або високий для продуктів та послуг ІКТ, що випускаються відповідно до цієї схеми [13].

Розглянемо детальніше законодавчий пакет ЄС з кібербезпеки (2017 р.). Так, у вересні 2017 року Європейська комісія та Високий представник ЄС із закордонних справ і політики безпеки опублікували спільне повідомлення для Європейського парламенту і Ради ЄС під назвою «Стійкість, стримування і захист: створення сильної кібербезпеки для ЄС» («Спільне спілкування»), яке стало частиною пакету документів ЄС, прийнятих на цю ж

## *International experience in the field of ensuring information security of person, society, state*

---

дату, спрямованих на забезпечення більш сильного реагування ЄС на кібератаки. Зокрема, Спільне повідомлення передбачає цілеспрямовані заходи, скеровані на: створення більшої стійкості ЄС до кібератак, краще виявлення кібернападів і посилення міжнародної співпраці у сфері кібербезпеки.

У документі викладені заходи, спрямовані на підвищення кіберстійкості ЄС, які наведено в наступних положеннях.

1. Швидке прийняття нового Регламенту ЄС, який реформує Агентство ЄС з кібербезпеки (ENISA), надаючи йому постійний мандат, і встановлює рамки сертифікації ЄС з ENISA. Ці рамки визначатимуть процедуру створення добровільних схем сертифікації кібербезпеки ЄС. Це обмежить адміністративні та фінансові витрати для підприємств, яким необхідно здійснювати декілька процесів сертифікації під час ведення бізнесу в ЄС (2.1).

2. Ухвалення спільної галузевої ініціативи Європейської комісії щодо визначення принципу «обов'язки по догляду», який може зменшити уразливість програмного забезпечення продукту і сприяти «безпеці за задумом» (2.2).

3. Повна та ефективна імплементація Директиви ЄС про безпеку мережних та інформаційних систем («Директива NIS») усіма державами-членами ЄС до 9 травня 2018 року. 13 вересня 2017 року Комісія ЄС також видала Повідомлення для підтримки ЄС. Зусилля держав-членів, спрямовані на надання кращих практик та рекомендацій щодо того, як директива NIS повинна діяти на практиці (2.3).

4. Швидка реалізація «Концепції» для транскордонного реагування на великі інциденти. «План» був представлений у Рекомендації ЄС і визначає цілі та способи співпраці між державами-членами ЄС, а також між державами-членами ЄС та відповідними інституціями ЄС, у відповідь на масштабні інциденти та кризові ситуації у сфері кібербезпеки (2.4).

5. Проведення оцінювання впливу для вивчення можливості стимулювання розробки та впровадження технології кібербезпеки в рамках пропозиції Комісії в 2018 році про створення мережі центрів компетенції в області кібербезпеки з Європейським центром досліджень і компетенцій в області кібербезпеки як центральної фігури (2.5).

6. Визнання пріоритетності кіберпросвіти в національних інформаційних кампаніях ЄС, включаючи кібербезпеку як частину національних навчальних програм з академічної та професійної підготовки ЄС (2.6).

7. Розробка єдиного порталу – єдиного в масштабах ЄС – який буде надавати інформацію про останні кіберзагрози і об'єднувати практичні поради та інструменти кібербезпеки для допомоги жертвам кібератак (2.7).

Таким чином, на законодавчому рівні декларуються дії, спрямовані на створення ефективного кіберстимування, які важко вважати, що вони виконані:

– впровадження вимог щодо закупівель, досліджень та фінансування проєктів ЄС для переходу до нового протоколу (IPv6) на рівні ЄС, одночасно заохочуючи держави-члени ЄС розглянути можливість виконання

## ***Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави***

---

добровільних угод з постачальниками послуг для активізації використання IPv6 (3.1);

– пропозиції Європейської Комісії для полегшення транскордонного доступу до електронних доказів (на початку 2018 року) (3.2);

– швидке прийняття нової запропонованої Директиви ЄС про боротьбу з шахрайством і підrobкою безготівкових платіжних засобів (3.3);

– новий розширений фокус Центру кіберзлочинності Європолу на кіберекспертизу та моніторинг «темної мережі» (3.4);

– впровадження недавно прийнятої структури для спільного дипломатичного реагування ЄС на зловмисну кібердіяльність («Кібердипломатичний інструментарій») (3.5);

– посилена фінансова підтримка національних та транснаціональних проєктів, спрямованих на поліпшення кримінального правосуддя в кіберпросторі (3.6);

– впровадження платформи освіти, пов'язаної з кібербезпекою. Для вирішення поточних проблем у сфері кібербезпеки та кіберзахисту (3.7) [14].

В той же час важко вважати, що наведені заходи принципово змінюють ситуацію в ЄС щодо посилення кібербезпеки. Однак, певно, відчуваючи це, Європейська Комісія опублікувала Пропозицію Комісії щодо покращення «Закону про кібербезпеку». Вона включає в себе: Пропозицію щодо змін в Положення про ENISA та про необхідність сертифікації кібербезпеки у сфері інформаційних та комунікаційних технологій («Закон про кібербезпеку»). Йдеться про створення Агентства ЄС з кібербезпеки, яке

матиме оперативну роль для «протидії конкретним загрозам», як «центру експертизи» з сертифікації кібербезпеки та підтримки держав-членів у виконанні законодавства ЄС. Новий орган має замінити нинішнє ENISA «з метою ефективної підтримки держав-членів, інституцій ЄС та інших зацікавлених сторін для забезпечення безпечного кіберпростору в Європейському Союзі» [15].

Значний вплив на можливості та готовність держав-членів до сприйняття нового в зазначеній галузі очікується, зокрема, від надання довгострокового стратегічного аналізу кіберзагроз та інцидентів. Це допоможе визначити нові тенденції, надасть авторитетні рекомендації та звіти з питань кібербезпеки, спрямованих на приватні організації та громадян, допоможе у проведенні експертизи та передового досвіду між державами-членами, а також забезпечить навчання та навчальні матеріали для національних органів влади та для діяльності CSIRT, як керівництво щодо поліпшення зрілості CSIRT відповідно до передового досвіду ЄС та міжнародних стандартів. Посилення навчань Cyber Europe і участь у запропонованому проєкті співробітництва у сфері кіберкриз може допомогти в досягненні одного ключового кордону для готовності ЄС, який полягає в наявності добре налагодженого і узгодженого плану на випадок великомасштабного транскордонного кіберінциденту. Очікується, що участь ENISA в розробці та реалізації політики ЄС в області сертифікації безпеки ІКТ позитивно, хоча і побічно, вплине на загальну готовність ЄС. Фактично,



## *International experience in the field of ensuring information security of person, society, state*

---

просування відповідних керівних принципів сертифікації, що підтримують визнані в ЄС схеми, не тільки підвищить рівень забезпечення властивостей безпеки продуктів і послуг ІКТ, але також буде стимулювати впровадження належного рівня безпеки. Очікується, що вплив цієї політики буде дуже далекосяжним, враховуючи широке коло зацікавлених сторін (від окремих покупців до операторів критично важливих інфраструктур).

Таким чином, ЄС має достатньо сучасне законодавство з кібербезпеки, яке, на жаль, неспроможне захистити його від кібератак та підтримувати кібербезпеку цього об'єднання з відомих нам причин. Так, в епоху інформаційного суспільства більшість проблем кібербезпеки викликана відставанням сучасної законодавчої бази від науково-технічного прогресу в галузі інформаційних технологій. За декілька останніх десятиліть відбулася така потужна технологічна революція в галузі використання комп'ютерів та телекомунікацій, яка принципово призвела до зміни та збільшення апаратного парку, а також суттєвого прискорення швидкості передачі даних, охоплення світового простору інформаційними наземними і мобільними комунікаційними мережами. Все це супроводжувалося збільшенням пропускної спроможності, взаємозв'язаності та швидкодії інформаційних систем.

Стрибокподібне збільшення пропускної спроможності інформаційних комунікацій та збільшення обсягів і швидкодії мережевої інфраструктури (місткості та швидкодії серверів) привело до широкого розповсюдження

хмарних технологій (парадигма, що передбачає віддалену обробку та зберігання даних). Саме хмарні технології надають користувачам мережі Інтернет доступ до комп'ютерних ресурсів сервера і використання програмного забезпечення як онлайн-сервісу, тобто якщо є підключення до Інтернету, то можна виконувати складні обчислення, опрацьовувати дані, використовуючи потужності віддаленого сервера. З хмарними технологіями пов'язані й тенденції переходу від конвенціональних моделей розробки та обслуговування програмного забезпечення до хмарних схем (передачі та обробки даних за схемою (користувач-постачальник) «точка-точка»), зокрема таких як «Програмне забезпечення як послуга» (SaaS, Software-as-a-Service), «Платформа як послуга» (PaaS, Platform-as-a-Service), «Інфраструктура як послуга» (IaaS, Infrastructure-as-a-Service). При цьому при проектуванні та експлуатації хмарних додатків не приділяється належної уваги питанням безпеки та конфіденційності [16].

Окрім хмарних технологій, які передбачають віддалену обробку та зберігання даних, технологічний прогрес в області ІКТ привів до широкого розповсюдження так званих розподілених технологій. Частина таких технологій дотепер ще не вийшла за рамки дослідницьких проєктів. До таких технологій належать The InterPlanetary File System (IPFS), яка є спробою організації інтернет-системи на технологічних принципах відмінних від тих, що існують [17], цілий клас Friend-to-friend (F2F) однорангових децентралізованих мереж – Freenet,

## *Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави*

---

GNUnet, Netsukuku і MANET [18]. Інші розподілені мережі широко розповсюдилися і використовуються в різних варіаціях, наприклад, файлообмінні мережі. Зокрема, до цього класу належать найбільш поширені мережі, що побудовані навколо централізованих і децентралізованих порталів, які призначені для користувача та засновані на файлообміні за протоколом «bittorrent». Існує цілий клас мереж, визначуваних як Darknet і спрямованих на анонімізацію своїх користувачів, що разом з обходом урядової цензури в різних країнах дозволяє використовувати ці мережі в кримінальних цілях (розповсюдження незаконного контенту, торгівля наркотиками і зброєю, скоєння фінансових злочинів) [19].

Розповсюдження різного роду розподілених мереж створило серйозну проблему, оскільки сильно ускладнюється атрибуція зловмисників, а відповідно обмежуються й засоби боротьби з ними. Для вирішення цієї проблеми вносилися різні законодавчі ініціативи, з яких, на наш погляд, найбільш цікавим стає використання досвіду з подолання фрагментації в світовому законодавстві, який був одержаний в результаті взаємодії різних ланок при боротьбі з морським піратством [20]. Так само в зазначеній роботі показано проблеми, з якими стикаються служби кібербезпеки при роботі з міжнародною злочинністю, зокрема у виявленні китайських ботнетів і джерел атак для різних країн.

Разом з появою і розповсюдженням розподілених мереж у сучасному інформаційному просторі декілька глобальних лідерів (Facebook, Google,

Alibaba, Amazon) концентрують дані не тільки свої й не тільки у себе, а також несуть людству нові глобальні ризики. Вони поступово перетворюються «на інтернет в інтернеті», що можна порівняти з тими ризиками, які виникають на рівні роботи транснаціональних корпорацій, коли їх транснаціональне положення потенційно дозволяє обходити Союзні (для ЄС) та національні закони [21]. Крім того, виникнення глобальних лідерів призвело до концентрації інформації в руках «великих гравців мережі» та централізації загальної інфраструктури, що значно підвищує уразливість, оскільки у разі доступу зловмисника до системи такого глобального гравця, його діяльність ставить під загрозу всю інфраструктуру системи [22]. Це робить можливими великомасштабні атаки і збільшує ризик значних збитків при критичних пошкодженнях інфраструктури таких систем. Слід відзначити, що істотною проблемою стає використання персональних даних користувачів, що збираються такими структурами. Тут важливим стає їх використання не тільки самими глобальними гравцями, але і делегування ними даних третім особам [23; 24]. Зауважимо, що сучасні ініціативи ЄС, про які йшлося вище, направлені саме на протидію цьому тренду. Це, зокрема, стосується «Загального регламенту про захист даних» (General Data Protection Regulation (GDPR)), який визначає яким чином повинні використовуватися зібрані персональні дані громадян ЄС [25]. При цьому дія регламенту розповсюджується на всі майданчики,

## *International experience in the field of ensuring information security of person, society, state*

---

що обслуговують громадян ЄС, незалежно від приналежності й географічного положення майданчика, на якому це відбувається. Впровадження регламенту зустрічає критику і протидію, що пов'язано з глобальним характером Інтернету. Так, деякі компанії йдуть з європейських майданчиків, для того, щоб уникнути дії GDPR. Проте це істотний крок в правильному напрямі до захисту приватності даних користувачів і організації відкритих і прозорих інтернет-сервісів [26]. Це знаходить підтримку в суспільстві, оскільки законодавству необхідно протистояти як поточним, так і майбутнім викликам, які ставить перед ним науково-технічний прогрес. На наш погляд, одним із наступних етапів технологічної революції стане широке розповсюдження додатків, що використовують збір і аналіз великих обсягів даних, систем штучного інтелекту і технологій Інтернету речей, що в поєднанні з сучасними підходами створює велику «поверхню атаки» і, відповідно, збільшить кількість потенційних погроз. Однією з серйозних загроз, на нашу думку, стає використання програмного забезпечення в системах BIOS, що потенційно дозволяє заражати комп'ютери, залишаючись поза увагою традиційних антивірусних програм [27].

Серед необхідних заходів слід виокремити позитивні практики та законодавчі ініціативи, які сприяють оздоровленню і збільшенню стійкості інформаційної сфери [28]. До таких, зокрема, належить заохочення переходу державних та недержавних структур до систем із відкритим початковим

кодом і використання ліцензійно-чистих відкритих форматів даних [29], що дозволяє не тільки підвищити стійкість роботи відповідних підрозділів, але й однозначно заощадити значні бюджетні кошти.

**Висновки.** Таким чином, процес становлення кіберзаконодавства в країнах-членах ЄС розпочався у 2001 році й досі набирає оберти, створюючи нове законодавство в цій галузі. Однак з позиції системного підходу більшість проблем кібербезпеки виникає через відставання сучасної законодавчої бази від науково-технічного прогресу. За декілька останніх десятиліть відбулася потужна технологічна революція в галузі використання комп'ютерів та телекомунікацій, яка привела до принципових змін та збільшення апаратного парку, суттєвого прискорення швидкості передачі інформації. Водночас саме стрімкий інформаційний прогрес спричинив проблему захищеності персональних даних через виникнення глобальних лідерів, що призвело до концентрації інформації в руках «великих гравців мережі» та централізації загальної інфраструктури. Це зробило можливими великомасштабні атаки та створило великі ризики значних збитків при критичних пошкодженнях інфраструктури таких систем. Тому, незважаючи на існуючу сучасну низку документів щодо кібербезпеки, остання досі залишається досить вразливою, незалежно від ступеня розробки і стану законодавства, виявляючи випереджаючі проблемні науково-технічні прогалини щодо підвищення якості та стану кібербезпеки в ЄС загалом.

## ***Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави***

### **Список використаних джерел**

1. Василенко М. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства / М. Василенко // Юридичний вісник. – 2018. – № 3. – С. 17–24.
2. Василенко М. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення / М. Василенко // Юридичний вісник. – 2018. – № 4.
3. Резолюція Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки» від 20 грудня 2002 р. № 57/239 [Електронний ресурс]. – Режим доступу : [http://www.un.org/ru/ga/second/57/second\\_res.shtml](http://www.un.org/ru/ga/second/57/second_res.shtml).
4. Женевська декларація принципів від 12 грудня 2003 р. [Електронний ресурс]. – Режим доступу : <http://www.rada.gov.ua>.
5. Туніська програма для інформаційного суспільства від 18 листопада 2005 р. [Електронний ресурс]. – Режим доступу : [https://informationsociety.wordpress.com/basics/wsis\\_outcomes/tp/](https://informationsociety.wordpress.com/basics/wsis_outcomes/tp/).
6. About ENISA / European Union Agency for Network and Information Security [Електронний ресурс]. – Режим доступу : <https://www.enisa.europa.eu/about-enisa>.
7. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union [Електронний ресурс]. – Режим доступу : <https://ec.europa.eu/digital-singlemarket/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity>.
8. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших [Електронний ресурс]. – Режим доступу : <https://clck.ru/FEMKX>.
9. EU cybersecurity initiatives working towards a more secure online environment / European Union [Електронний ресурс]. – Режим доступу : <https://clck.ru/FEMKo>.
10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. – 2016. – L. 194. – P. 1–30.
11. Tauwhare, R. (2016). Improving cybersecurity in the European Union: the Network and Information Security Directive. Journal of Internet Law, 19(2), 1–12.
12. The EU's Revised Cybersecurity Strategy [Електронний ресурс]. – Режим доступу : [https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C47\\_bdk\\_etal.pdf](https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C47_bdk_etal.pdf).
13. Proposal for a regulation of the European Parliament and of the Council on ENISA, the «EU Cybersecurity Agency», and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification («Cybersecurity Act») [Електронний ресурс]. – Режим доступу : <https://clck.ru/FEMLa>.
14. Renewed Cybersecurity Strategy: European Parliament and Council Joint Communication ‘Resilience, Deterrence and Defence: Building strong cybersecurity for the EU’ (JOIN (2017) 450) [Електронний ресурс]. – Режим доступу : <https://clck.ru/FEMLM>.
15. Commission Proposal for a Cybersecurity Act: Proposal for a Regulation on ENISA, the «EU Cybersecurity Agency», and on Information and Communication Technology cybersecurity certification («Cybersecurity Act») – COM (2017) 477 [Електронний ресурс]. – Режим доступу : <https://clck.ru/FEMLa>.
16. Saleem M. Q., Jaafar J., Hassan M. F. Model driven security frameworks for ad-

## *International experience in the field of ensuring information security of person, society, state*

---

addressing security problems of Service Oriented Architecture // 2010 International Symposium on Information Technology. – IEEE, 2010. – Т. 3. – С. 1341–1346.

17. Benet J. Ipfs-content addressed, versioned, p2p file system // arXiv preprint arXiv: 1407.3561. – 2014.

18. Rogers M., Bhatti S. How to disappear completely: A survey of private peer-to-peer networks // RN. – 2007. – Т. 7. – № 13. – С. 1.

19. Huang K., Siegel M., Stuart M. Systematically Understanding the Cyber Attack Business: A Survey // ACM Computing Surveys (CSUR). – 2018. – Т. 51. – № 4. – С. 70.

20. Stahl W. M. The uncharted waters of cyberspace: applying the principles of international maritime law to the problem of cybersecurity // Ga. J. Int'l & Comp. L. – 2011. – Т. 40. – С. 247.

21. Moore M., Tambini D. (ed.). Digital dominance: the power of Google, Amazon, Facebook, and Apple. – Oxford University Press, 2018.

22. Simon P. The age of the platform: How Amazon, Apple, Facebook, and Google have redefined business. – BookBaby, 2011.

23. Haucap J., Heimeshoff U. Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization? // International Economics and Economic Policy. – 2014. – Т. 11. – № 1–2. – С. 49–61.

24. Petrescu M., Krishen A. S. Analyzing the analytics: data privacy concerns. – 2018.

25. Denley A., Foulsham M., Hitchen B. GDPR: How to Achieve and Maintain Compliance. – Routledge, 2019.

26. Raul A. C. (ed.). The privacy, data protection and cybersecurity law review. – Law Business Research Limited, 2018.

27. Furtak A. et al. Bios and secure boot attacks uncovered // The 10th ekoparty Security Conference. – 2014.

28. Herala A. et al. Strategy for Data: Open it or Hack it? // Journal of Theoretical and Applied Electronic Commerce Research. – 2019. – Т. 14. – № 2. – С. 33–46.

29. Schmidhuber L., Stütz S., Hilgers D. Outcomes of open government: Does an online platform improve citizens' perception of local government? // International Journal of Public Sector Management. – 2019.

---

**Аннотация.** В статье рассматривается становление кибербезопасности в ЕС и странах-членах на законодательном уровне с позиций системного подхода. Выявлены проблемные аспекты повышения качества и состояния кибербезопасности. Исследовано влияние состояния законодательства стран-членов ЕС на кибербезопасность. Также рассмотрен процесс развития ИКТ и показано, как новые технологии создают новые вызовы.

**Ключевые слова:** кибербезопасность, киберустойчивость, инструменты регулирования, законодательство ЕС, инновационные технологии.

**Abstract.** The article deals with the issues of establishing cybersecurity in the EU and its member-states at the legislative level as viewed from the point of a systematic approach. The authors identified problematic aspects of improving cybersecurity quality and conditions. They analyzed the impact of the EU member states legislation on cybersecurity. The article as well considers the process of ICT development and presents the ways of creating new challenges by means of new technologies.

**Key words:** cybersecurity, cyber resilience, regulatory instruments, EU legislation, innovations.