УДК 341.4
DOI https://doi.org/10.32782/2524-0374/2023-12/120

ОКРЕМІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄС

SOME ASPECTS OF EU INFORMATION SECURITY

Гроза Д.В., студентка IV курсу факультету прокуратури
Національний юридичний університет імені Ярослава Мудрого

Стаття присвячена дослідженню окремих аспектів інформаційної безпеки Європейського Союзу, а саме боротьби з проявами кібератак. Було акцентовано увагу на тому, що не вироблено єдиного поняття кібербезпеки ані на владному рівні ЄС, ані на науковому рівні. В аспекті цього автором досліджено окремі поняття запропоновані науковою спільнотою. Також автором ставиться питання, щодо складових компонентів інформаціної безпеки, тоді як Європейське агентство з мережевої та інформаційної безпеки ЄС вважає, кібербезпеку та інформаційну безпеку, тотожними поняттями. До того ж, вивчено історико-правовий розвиток інформаційної безпекової політики ЄС та сформульовано висновки. У розрізі цього проаналізовано окремі кібер-інциденти, що стали поштовхом до розвику нормативно-правового забезпечення країн-членів у сфері кібербезпеки. Вивчено нормативно-правові акти, що регулюють сферу кібербезпеки країн-членів ЄС на національному рівні та певні акти наднаціонального рівня ЄС. Надано оцінку безпековій політиці ЄС та наголошено на її окремих недоліках, зокрема в контексті «швидкого реагування» – повідомленнь відповідним органам про атаку, включаючи санкції за порушення цих правил.

Висвітлено класифікацію кіберзагроз, що становлять небезпеку для інформаційних систем у 2023 році, а також визначено період в який кібезлочинці здійснили найбільше кібератак, саме коли світ стикнувся з пандемією COVID-19. Варто констатувати, що ці дії кібершпигунів збільшили уразливість інформаційної безпеки майже для всіх країн світу, що змусило державні органи оцінити наявні ризики та реформувати політику інформаційної безпеки.

Визначено «європейський індекс безпеки» станом на 2021 рік європейських країн, дослідивши, як кожна країна вирішує питання кібербезпеки та наскільки поширені хакерство та онлайн-шахрайство серед жителів країн-членів ЄС. Розглянуто нову стратегію кібербезпеки ЄС на 2020–2025 роки. Зважено позитивні та негативні сторони даного акту, які впливатимуть на реагування кібаератак та регенерацію після них.

Ключові слова: інформація, інформаційна безпека, кібербезпека, кібератаки, національна безпека, кібервійна.

The paper is devoted to the study of certain aspects of the information security of the European Union, namely the fight against manifestations of cyber attacks. Attention was focused on the fact that a single concept of cyber security has not been developed either at the EU governmental level or at the scientific level. In this aspect, the author researched certain concepts proposed by the scientific community. The author also raises a question about the components of information security, while the European Agency for Network and Information Security of the EU considers cyber security and information security to be identical concepts. In addition, the historical and legal development of the information security policy of the EU was studied and conclusions were formulated. In this context, individual cyber incidents were analyzed, which became an impetus for the development of regulatory and legal support of member countries in the field of cyber security. The normative legal acts regulating the sphere of cyber security of the EU member states at the national level and certain acts of the supranational level of the EU have been studied. An assessment of the EU's security policy is given and its individual shortcomings are emphasized, in particular in the context of «quick response» – notifications to the relevant authorities about an attack, including sanctions for violations of these rules.

The classification of cyberthreats that pose a danger to information systems in 2023 is highlighted, as well as the period in which cybercriminals carried out the most cyberattacks, precisely when the world was faced with the COVID-19 pandemic. It is worth stating that these actions of cyber spies increased the vulnerability of information security for almost all countries of the world, which forced the state authorities to assess the existing risks and reform the information security policy.

The 2021 «European Security Index» of European countries was determined by examining how each country deals with cyber security and how common hacking and online fraud are among residents of EU member states. The new EU cyber security strategy for 2020–2025 was considered. We have weighed the positive and negative sides of this act, which will affect the response of kibaera attacks and the regeneration after them.

Key words: information, information security, cyber security, cyber attacks, national security, cyber warfare.

Вступ. Національна безпека складає основу життєздатності будь-якої країни. Політика національної безпеки, яку провадять уряди, має на меті забезпечити стабільну безпеку громадян, захистити державу від зовнішніх та внутрішніх загроз різного характеру: політичного, економічного, екологічного, соціального та інформаційного. Безумовно, рівень їх впровадження залежить від ресурсного потенціалу держави та безпосередньо ефективності запропонованих векторів розвитку.

З початком повномасштабного вторгнення рф на територію України реалізація єдиної інформаційної політики є одним з пріоритетів національної безпеки. Тому що наразі атаки являють собою не тільки «проникнення» в комп'ютерні мережі, ракетні атаки на критичну інфраструктуру, а й інформаційний вплив на психіку громадян, що виявляється у певних маніпуляціях, погрозах, поширення дезінформації серед населення тощо.

Тож, наявність якісної нормативної бази має відповідати вимогам сучасності, регулювати діяльність суб'єктів інформаційної безпеки на всіх рівнях, регламентувати їх права, обов'язки, юридичну відповідальність за порушення норм. Також, визначати засоби протидії загрозам інформаційної безпеки, включаючи превентивні заходи.

У попередніх наших роботах були проведені дослідження нормативного забезпечення окремих аспектів національної безпеки країн-членів ЄС та акцентовано увагу на їх своєчасному реагуванню. Зокрема, присвячено увагу окремим аспектам демографічної безпеки, питанням щодо права на захист, зброї, оборонної сфери ЄС тощо [1; 2; 3; 4].

Виклад основого матеріалу. В умовах сьогодення інформаційні технології пронизують всі сфери життя індивіда. Вони дозволяють проводити різні досліди без участі людини, створювати різноманітні моделі та конструкції для розвитку науки, забезпечувати швидкий обмін даними тощо. Ступінь розвиненості інформаційних технологій країни позначається на всіх сферах її розвитку, в тому числі, яку роль вона відіграє на міжнародній арені.

У важливості та необхідності ІТ-технологій в епоху інформації і науки ні в кого не виникає сумнівів. Як і будь-яке інше досягнення науково-технічного прогресу, досягнення у сфері ІТ-технологій несуть (одночасно з перевагами) й певний перелік загроз: віруси, кібератаки, шахрайство в Інтернеті, дезінформація та ін. Для юридичної науки особливо актуально постає питання про вироблення механізмів та засобів правового регулювання захисту даних, попередження проявів кібератак та інших загроз кібербезпеці держави.

У зв'язку з цим варто детальніше розглянути таке явище як кібератака. Кібератака являє собою дестабілізацію комп'ютерних систем, доступу до Інтернету державних установ, створення безладу в різних секторах життєдіяльності країни. Стосунки суб'єктів геополітики, їх політичне протистояння нерідко знаходить своє продовження в Інтернеті у вигляді кібервійни[1]. Адже саме такий вид недобросовісної конкуренціїможе завдати значної шкоди економіці іншої держави, так би мовити «заморозити (дестабілізувати) життєдіяльність конкурента на певний час». Тому, кібербезпека на сьогоднішній день має посідати чільне місце національної безпеки країн ЄС.

Перейдемо до визначення дефініції «кібербезпека». У 2012 році Європейське агентство з мережевої та інформаційної безпеки ЄС (National Cyber Security Strategies) опублікувало посібник (Practical Guide on Development and Execution) [6], який мав на меті надати корисні та практичні рекомендації громадськості та зацікавленим сторонам щодо розробки, впровадження та підтримки стратегії кібербезпеки. Але, щодо визначення терміну «кібербезпека» в посібнику зазначалось таке: «Не існує загальноприйнятого чи прямолінійного визначення кібербезпеки. Порівнюючи це з «інформаційною безпекою», деякі особи вважають це дублюванням, тобто тим самим. Або вони можуть розглядати інформаційну безпеку як зосереджену на захисті конкретних окремих систем та інформації в організаціях, тоді як кібербезпека розглядається як зосереджена на захисті інфраструктури та мереж ІСІ[2]». Ми частково погоджуємося з такою думкою, адже досить складно виробити єдине поняття, розрізняються підходи не тільки до стратегій, яким слідують держави, а й до змісту плану дій.

Сучасні технології знаходяться постійно на шляху вдосконалення та розвитку. Разом з ними трансформуються способи кібератак. Так само, йде постійне напрацювання та оптимізація дефініцій кібербезпеки. Варто зазначити, що поняття «кібербезпека» не має усталеного законодавчого закріплення. На нашу думку, проблемі визначення поняття «кібербезпека» буде постійно приділятися увага правової наукової спільноти. На теперішній час, науковцями запропоновано багато визначень, тому вважаємо за необхідне навести приклади окремих з них.

Деякі дослідники розмежовують поняття інформаційної безпеки та кібербезпеки, аргументуючи, що інформаційна безпека має на меті забезпечити захист будь-яких важливих даних, натомість кібербезпека сконцентрована на цифровій інформації [8]. Маємо намір не погодитися з такою думкою, адже вважаємо, що кібербезпека є невід'ємною частиною інформаційної безпеки (тобто більш ширшим поняттям). Окремі вчені розглядають кібербезпеку як певний статичний стан суспільства в якому відсутня небезпека, стан захищеності життєво важливих інтересів індивідів та держави [9]. Або ж пов'язують це напряму з діяльністю людини, суспільства та держави, що виражається в певних превентивних діях [10].

Вважаємо, що в цілях нашого дослідження найповніше розкриває сутність дефініції «кібербезпека» Баранова О. А. На його думку, кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [12].

В межах нашого дослідження вважаємо за необхідне окремо розглянути деякі історичні події, що мали вплив на подальший розвиток нормативного забезпечення кібербезпеки в ЄС. Поступове залучення Європейського Союзу до питань кібербезпеки було сформоване деякими кіберінцидентами, які були безпрецедентними викликами безпеці ЄС і суттєво вплинули на те, як держави-члени сприйняли кібердомен.

Почнімо з того, що в 2007 році органи влади Естонії, медіа-канали, банки та комунікація інфраструктури стали жертвами тривалої кібератаки. На той час Естонія, як член НАТО, так і член Європейського Союзу, була однією з найбільш розвинутих країн у Європі та загалом технічно компетентною, яка швидко розвивала послуги «електронного уряду». Також, країна використовувала інтернет-технології голосування, освіти, безпеки та банківської справи [12].

Атаки на ІТ-інфраструктуру Естонії назвали першою в світі кібервійною [13]. Вона стала першим відомим випадком атаки на цілу країну шляхом масового кібернаступу. Дослідники вказують, що «це був перший раз, коли тривалий, масовий і політично вмотивований електронний напад було розпочато, щоб розсіяти хаос для всієї цифрової інфраструктури країни» [14].

Варто зазначити, що до нападу 2007 року, Естонія фактично не переймалася щодо національної безпеки, розвиваючи цифрове суспільство, оскільки, не прорахувала ризиків атаки на нього. Саме цей випадок став прикладом для світу, показавши, що ІТ-системи можуть бути використані як альтернативний спосіб поширення терору та дезорганізації країни [12].

Загалом кібератаки, які були направлені на уряд Естонії, були досить значними, але й вони не призвели до розробки спільної стратегії кібербезпеки на рівні ЄС. Питання кібербезпеки поступово зацікавлювали саме країни-членів ЄС та провокували відповідні дискусії в основному на національному рівні. Вважаємо, що з урахуванням специфіки розподіли компетенції між наднаціональним рівнем (ЄС) та національним (держави-члени), недостатнім рівнем довіри до інститутів ЄС та між самими державами-членами у таких чутливих питаннях національної безпеки, країни-члени фактично залишили вирішувати це питання на національному рівні.

Зокрема, одна з перших країн-членів ЄС, яка запровадила план дій щодо кібербезпеки була Німеччина. У 2005 році Німеччина прийняла Національний план щодо «Захисту інформаційної інфраструктури (NPSI)». NPSI була першою національною стратегією, пов'язаною з ІТ-безпекою Німеччини [15].

Вслід за Німеччиною, Швеція представила «Стратегію покращення безпеки Інтернету в Швеції» [16] і помітно стала першою державою-членом ЄС, яка опублікувати широку національну стратегію кібербезпеки після кібератаки в Естонії. Зокрема, сама Естонія у 2008 році сформувала стратегію, прагнувши зменшити вразливість кіберпростору нації в цілому [17].

У 2008 році Фінляндія сформувала національний план кібербезпеки [18]. Фінляндія сприймає кібербезпеку як «проблему безпеки даних і як питання економічного характеру значення, яке тісно пов'язане з розвитком інформаційного суспільства» [19]. У Словаччині Національна стратегія інформаційної безпеки (NSIS) була впроваджена до 2013 року [20].

Протягом наступних років все більше і більше країнчленів ЄС запровадили національні стратегії та інші акти, що регламентують національну політику у сфері кібербезпеки. Наприклад, у лютому 2011 року Національне агентство з кібербезпеки Франції (ANSSI) опублікувало Французьку стратегію кіберзахисту та кібербезпеки [21].

---

[1] **Кібервійна** – це масова скоординована цифрова атака на уряд з боку іншої сторони або великих груп осіб. Це дії держави, спрямовані на проникнення в комп'ютери та мережі іншої нації з метою заподіяння шкоди або спричинення збою [5].

[2] Інститути спільного інвестування (ІСІ) це інвестиційні фонди, які провадять діяльності зі спільного інвестування – об'єднання (залучення) грошових коштів інвесторів з метою отримання прибутку від вкладення їх у цінні папери інших емітентів, корпоративні права та нерухомість [7].

Інші країни-члени, такі як Польща [22], Італія [23], Угорщина [24] сформували національні стратегії кібербезпеки у 2013 році.

У 2008 році Європейська Комісія розпочала публічні консультації щодо мережі та політики інформаційної безпеки в Європі. У 2009 році Європейська Комісія підкреслила важливість безперебійного функціонування комунікаційної інфраструктури для європейської економіки і суспільства та закликала до дій для захисту цієї критичної інформаційної інфраструктури, зробивши ЄС більш підготовленим і стійким до кібератак і збоїв [25].

Атака на енергомережу України у 2015 році є першою публічно визнаною кібератакою на енергетичний сектор, яка спричинила серйозне відключення електроенергії [26]. Це також підкреслює важливість кібербезпеки саме в енергетичному секторі, оскільки він становить одну з найважливіших національних інфраструктур. Кібер-інциденти, які мають місце в останні роки, викликають більш серйозне занепокоєння про безпеку в кіберсфері на рівні ЄС і посилюють інтерес до зміцнення співпраці держав-членів ЄС.

Приклади таких інцидентів – це серйозні витоки даних (DoS-атаки на медіа-платформи, таких як Twitter і Facebook [12], згадані вище атаки на інфраструктуру у Фінляндії, та уряд Німеччини за допомогою зловмисного програмного забезпечення, яке проникло в обидва МЗС і Міноборони, а також втручання у вибори та кібершпигунство Норвегії [27], Данії [28], Нідерландів [29] та Італії [30].

Вважаємо, що внаслідок декількох серйозних кібератак, країни-члени постраждали саме через відсутність співпраці та спільної позиції щодо питань кібербезпеки на рівні Союзу. Інциденти зростають та стають все більш складними, загрожуючи безпеці та економіці, реагування на кібератаки були фрагментарними та недостатньо послідовними, щоб впоратися з кібервикликами.

Надавши окремі історичні приклади можна зробити проміжний висновок, що кібератаки спричинили великий вплив на формування стратегії кібербезпеки ЄС. Це кинуло виклик державам-членам ЄС і спонукало їх адаптувати свою реакцію до реальної зростаючої цифровізації, взаємопов'язаності світу та складних кібератак, що швидко розвиваються, запровадити нові підходи та заходи для зміцнення приватно-державного партнерства тощо.

ENISA *(Європейське агентство з питань мережевої та інформаційної безпеки)* оцінює, що в найближчі роки головними тенденціями в ландшафті кіберзагроз можуть бути: зростання складності та витонченості кібератак, тобто, зловмисники ставатимуть все більш і більш просунутими, а інфраструктура для кібердій буде більше використовувати анонімізацію; шифрування та ухилення від виявлення правоохоронними органами; перетворення фінансової вигоди на основний мотив для зловмисників у кібернетичному просторі, як правило, за підтримки держави-дестабілізатора. До того ж, ENISA стверджує, що безпека від кіберризиків міцно пов'язується з набуттям навичок і здібностей, з навчальними та освітніми програмами в організаціях по всьому ЄС [31].

Як уже зазначалося вище, держави-члени формували стратегії та політику інформаційної безпеки самостійно, зокрема, через відсутність взаємної довіри та неузгодженості між членами. Реакція ЄС має бути комплексною та базуватися на узгодженому наборі дій поєднання внутрішньої та зовнішньої політики. ЄС має стати одним цілим, щоб бути сильним гравцем у кіберпросторі. Обґрунтуванням цього можуть слугувати статистичні данні.

Компанія ESET (міжнародний розробник програмного забезпечення) перевірила «європейський індекс безпеки» станом на 2021 рік європейських країн, дослідивши, як кожна країна вирішує питання кібербезпеки та наскільки поширені хакерство та онлайн-шахрайство серед жителів держави. Та склала рейтинг країн з найкращим та найгіршим рівнем безпеки [32].

Згідно з дослідженням, компанія оцінювала кожну країну за 10-бальною шкалою. При оцінюванні враховувалися такі фактори: ступінь вразливості до потенційних атак, зацікавленість країни у розвитку кібербезпеки, нормативно-правове забезпечення стосовно кібербезпеки та кількість осіб, які стали жертвами кібератак.

Очолює рейтинг Португалія як країна з найбільш безпечним кібернетичним простором, її оцінка склала – 8,21 з 10 балів. Ця країна має низьку кількість людей, які стали жертвами зловмисного програмного забезпечення, хакерства в соціальних мережах, шахрайства в онлайн-банкінгу та крадіжки особистих даних. Також, слід відмітити як активне вдосконалення безпеки інформаційного простору так і запроваджену національну стратегію у цій сфері, рівень забезпечення конфіденційності, стан критичної інфраструктури.

«Срібло» отримала Литва, її оцінка складає 7,99 з 10. Литва є прихильником кібербезпеки, та віддано формує безпечний онлайн-простір для своїх громадян.

Закриває трійку лідерів Словаччина, вона отримує 7,21 з 10 балів. Ця країна добре позиціонується з точки зору ризику, фактору, який визначає, чи сайти та служби піддаються ризику через відсутність засобів захисту.

Стосовно іншихдержав-членів ЄС, то вони були оцінені так: Греція – 7,03; Іспанія – 6,82; Естонія – 6,75; Латвія – 6,20; Фінляндія – 6,09; Данія – 6,08; Словенія – 6 ,05; Італія – 5,93; Німеччина – 5,89; Польща – 5,87; Хорватія – 5,66; Угорщина – 5,61; Швеція – 5,59; Нідерланди – 5,47; Ірландія – 5,36; Люксембург – 4,40; Бельгія – 4,37; Франція – 4,36; Австрія – 3,80, Румунія – 3,27. Ці європейські країни були оцінені за факторами, що охоплюють їх реакцію на проблеми кібербезпеки, ризики, які існують для громадян, коли вони знаходяться в Інтернеті.

Такі дані вказують на недосягнення спільного курсу розвитку та ведення спільної політики країн-членів, що є дійсно проблемою для ЄС, адже коли кібератака вражає одну з країн ЄС (слабшу за своєю кіберполітикою), вона з легкістю може розширити своє поле ураження та повністю дестабілізувати всю європейську спільноту.

Далі з'ясуємо класифікації кіберзагроз. Говорячи про них, ENISA у 2023 році опублікувала Ландшафт загроз, що становлять небезпеку для ЄС [33].

1) Програми-вимагачі. Тип зловмисної атаки, коли кіберзлочинці шифрують дані організації та вимагають плату за відновлення доступу. Про важливість і вплив загрози програм-вимагачів також свідчить низка відповідних політичних ініціатив у Європейському Союзі (ЄС) та в усьому світі.

2) Шкідливе програмне забезпечення. Шкідливе програмне забезпечення, призначене для виконання несанкціонованого процесу, який матиме негативний вплив на конфіденційність, цілісність або доступність системи. Примітно, що, незважаючи на зниження в 2022 році, як раніше підкреслювалося в доповіді за 2022, початок 2023 року став свідком відродження інцидентів, пов'язаних з цим типом загрози.

3) Соціальна інженерія. Соціальна інженерія охоплює широкий спектр заходів, які намагаються використовувати людську помилку з метою отримання доступу до інформації або послуг. Зловмисники використовують різні форми маніпуляції, щоб ввести особу в оману та передати конфіденційну або секретну інформацію. Користувачі можуть бути заманені, щоб відкрити документи, файли або електронні листи, відвідати веб-сайти або надати доступ до систем або послуг.

4) Порушення та витік даних. Витік даних – це навмисна атака, здійснена кіберзлочинцем з метою отримання несанкціонованого доступу до конфіденційних або захищених даних.Зазначається, що на сьогодні почастішали випадки витоку даних у сфері охорони здоров'я.

5) Розподілені атаки типу «відмова в обслуговуванні» (DDoS). Атаки, що перешкоджають користувачам

мережі або системи отримати доступ до відповідної інформації, послуг та інших ресурсів. За останні кілька років з початку COVID-19 і вторгнення росії в Україну суттєво змінився ландшафт загроз із збільшенням спонсорованих державою атак на критичну інфраструктуру країн.

6) Інтернет-загрози. Загрози доступу до Інтернету стосуються навмисних або ненавмисних збоїв мережі Інтернет або електронних комунікацій, які призводять до його відключень. Збої в роботі Інтернету можуть бути пов'язані з від'єднанням від мережі, відключеннями електроенергії, кібератаками, технічними проблемами, природними явищами і військовими діями.

7) Інформаційні маніпуляції. Ці дії описують як незаконну модель поведінки, яка загрожує або може негативно вплинути на цінності, процедури та політичні процеси (підроблені фото, відео, поширення неправдивої інформації (наклепу) про політичних діячів). Така діяльність носить маніпулятивний характер, ведеться навмисним і скоординованим чином.

8) Атаки на ланцюги поставок. Вона спрямована на відносини між організаціями та їх постачальниками. Атака вважається як такою, коли вона складається з комбінації принаймні двох атак; більш конкретно, перша атака йде на постачальника, який потім використовується для атаки на ціль, щоб отримати доступ до своїх активів. До прикладу, російські хакери зосереджені на використанні програм-вимагачів для атак на ланцюжки поставок як в Україні, так і в європейських країнах, які використовуються для надання зброї та гуманітарної допомоги на підтримку українських військових.

Виходячи з цього, можна прослідкувати, що кіберзлочинці здійснили найбільше атак, коли світ стикнувся з пандемією COVID-19, що в свою чергу, відкрила нові можливості для кібершпигунів та збільшила уразливість інформаційної безпеки майже для всіх країн світу. Більше того, кібершпигунам властиво поєднувати ці типи атак одночасно, наприклад, здійснити напад на інфраструктуру і розсіяти дезінформацію серед населення. Це значно ускладнює процес регенерації для держави, адже важливо нормалізувати роботу інфраструктури, забезпечити її захист та донести правдиву інформацію до населення.

З огляду на події, що розгорталися навколо ЄС, першим кроком до створення та розвитку системи кібербезпеки ЄС стало прийняття стратегії кібербезпеки в 2013 році. Стратегія визначила досягнення кіберстійкості та розвиток промислових і технологічних ресурсів для кібербезпеки як її ключові цілі. Директива про безпеку мережевих та інформаційних систем в ЄС (*Directive (EU) 2016/1148*), є першим актом права ЄС щодо кібербезпеки. Вона передбачила правові заходи для підвищення загального рівня кібербезпеки в ЄС, зосереджуючись на захисті критичної інфраструктури [34].

Щоб відреагувати на зростаючі загрози, пов'язані з цифровізацією та напливом кібератак, Комісія подала пропозицію замінити Директиву NIS і, таким чином, посилити вимоги безпеки, оптимізувати зобов'язання щодо звітності та запровадити більш жорсткі вимоги, а саме, наглядові заходи та суворіші вимоги до виконання, включаючи узгоджені санкції в ЄС.

Відтоді було прийнято нову стратегію кібербезпеки ЄС на 2020–2025 роки [35], яка, серед багатьох речей, пропонує перегляд Директиви NIS, ухвалення нової Директиви щодо стійкості критичних об'єктів (*Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*) (CER), створення мережі центрів безпеки (SOC) та нові заходи для зміцнення інструментарію кібердипломатії ЄС.

Це відповідає пріоритетам Комісії – зробити Європейський Союз придатним до цифрової ери та побудувати готову до майбутнього економіку, яка працюватиме на громадян.

Ландшафт загроз суттєво змінився з моменту прийняття Директиви NIS у 2016 році, і сфера дії Директиви потребує оновлення та розширення, щоб відповідати поточним ризикам і майбутнім викликам, одним із таких завдань є забезпечення безпеки технології 5G. До того ж, її імплементація державами-членами виявила властиві закони в певних положеннях або підходах, наприклад, нечітке розмежування сфери застосування директиви.

Врегулювання інформаційної безпеки як на практиці так і в теорії з використанням новітніх технологій, досить складний процес, адже неможливо на 100% прорахувати всі ризики, убезпечити об'єкти критичної інфраструктури від неочікуваних атак, що і є основною проблемою для ЄС, нормативне забезпечення не встигає за розвитком інформаційних технологій.

Суд ЄС у своєму рішенні у справі C-58/08 *(Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform)* [36] вказав на необхідність встановлення чітких спільних правил щодо сфери застосування Директиви NIS та гармонізації правил з управління ризиками кібербезпеки та звітування про інциденти. Поточні розбіжності в цій сфері на законодавчому, наглядовому, національному та європейському рівнях є перешкодами для внутрішнього ринку, оскільки суб'єкти, які займаються транскордонною діяльністю, стикаються з різними, і, можливо, дублюючими нормативними вимогами та/або їх застосуванням на шкоду здійснення своїх свобод заснування та надання послуг.

У зв'язку з недосконалістю Директиви (NIS), 16 грудня 2020 року Комісія представила пропозицію (*Proposal for Directive (EU) 2016/1148*) щодо заходів на загальному рівні кібербезпеки Союзу (NIS2), яка б скасувала і замінила існуючу [37].

Правовою основою як для (NIS), так і для запропонованої (NIS2) є стаття 114 Договору про функціонування Європейського Союзу [38], метою якого є створення та функціонування внутрішнього ринку шляхом посилення заходів щодо наближення національних правил.

Запропоноване розширення сфери застосування, фактично зобов'яже більше суб'єктів і секторів до вжиття заходів, що сприятиме підвищенню рівню кібербезпеки в Європі в довготривалій перспективі.

Загалом пропозиція, визначена Директиві (NIS2) ставить перед собою три загальні цілі:

1) підвищення рівня кіберстійкості повного набору діючих підприємств Європейського Союзу в усіх відповідних секторах, запровадивши правила, які зобов'яжуть всі державні та приватні організації внутрішнього ринку приймати адекватні заходи кібербезпеки. Тобто, встановлюється, що всі середнього розміру і великі підприємства, що працюють у секторах, охоплених системою NIS2, повинні дотримуватися правил безпеки, викладених у пропозиції;

2) зменшення неузгодженості у стійкості внутрішнього ринку в секторах на які поширюється дія директиви, шляхом подальшого узгодження: а) безпеки та вимог до звітності про інциденти; б) положення, що регулюють національний нагляд та виконання.

Крім того, пропозиція передбачає двоетапний підхід до звітування про інциденти у сфері кібербезпек. Постраждалі компанії мають протягом 24 годин з моменту, коли їм вперше стало відомо про інцидент, подати звіт щодо атаки та реагування. Якщо ж компанії не подають звітність, то до них можуть бути застосовані санкції: негрошового характеру (Non-monetary Penalties) (додержання інструкцій, накази про проведення аудиту безпеки, сповіщення про загрози клієнтам компанії), адміністративні санкції (штрафи для різних секторів господарювання від 7 до 10 млн євро) та кримінально-правові санкції (притягати керівників організацій до персональної відповідальності, якщо після кіберінциденту доведено грубу недбалість) [39];

3) поліпшення рівня спільного усвідомлення ситуації та колективної здатності до реагування: а) вживання заходів для підвищення рівня довіри між компетентними органами, шляхом обміну додатковою інформацією; і б) встановлення правил і процедури реагування у разі масштабного інциденту чи кризи.

На нашу думку, нові правила здатні вдосконалити те, як ЄС запобігає, обробляє та реагує на масштабні інциденти і кризи у сфері кібербезпеки шляхом запровадження чіткої відповідальності (розподіл обов'язків, визначення зони відповідальності кожного держави-члена), належного планування між державами-членами та більшої співпраці між країнами-членами. Директива започаткує кризове управління рамок ЄС, які вимагають від держав-членів прийняти план і призначити національні компетентні органи, відповідальні за участь у реагуванні на інциденти та кризи на рівні ЄС.

Проте, маємо певні побоювання, як вже було зазначено, що нормативне забезпечення ЄС не завжди встигає врегулювати та відреагувати на появу нових інформаційних технологій. Враховуючи бюрократичне життя Європи, ми вважаємо, буде досить складно слідувати якісно та послідовно цим стандартам в разі реальної небезпеки та серйозній загрозі витоку даних.

Отже, сформулюємо основні висновки та рекомендації. Кібератаки не мають кордонів, обмежитись одним комплексним документом для нормативного регулювання протидії їм неможливо. Зміцнення стійкості інформаційних технологій має бути пріоритетом для ЄС. Без достатнього рівня безпеки будь-яка установа може втратити свої дані та, відповідно, власний авторитет. Однак ефективна кібербезпека не може бути скоординована силами одного уповноваженого суб'єкта , це є виважена, комплексна, всебічно розглянута, дієва реакція на загрозу. Перш за все, кібербезпека є колективною відповідальністю, і кожна держава-член повинна запровадити комплекс якісних практик для ефективного підвищення стійкості на рівні ЄС.

Кібербезпека не завжди передбачає успішну роботу спеціальних служб, робочих груп, перш за все, це робота всіх учасників: органів мережевої та інформаційної безпеки, правоохоронних органів, як на національному рівні, так і на рівні Європейського Союзу.

Крім того, сильна кібер-спільнота залежить від розвитку кібер-дипломатії, яка потребує постійного вдосконалення зважаючи на стрімкий розвиток ІТ. До того ж, суттєво впливає кібер-обізнаність громадян. Щоб протистояти не тільки на глобальному рівні кіберзагрозам, але й на особистісному, варто весь час підвищувати свою обізнаність в кіберпросторі, сюди входить і парольна безпека, використання лише ліцензійного програмного забезпечення, безпечних месенджерів.

Можна констатувати, що ЄС стоїть на вірному шляху та розвиває свій потенціал у сфері кібербезпеки та діджіталізації, максимально намагаючись як впроваджувати цифрові технології у всі сфери життєдіяльності європейського суспільства так і ефективно захищати їх.

ЛІТЕРАТУРА

1. Бойчук Д. С., Гроза Д. В. Міграційні кризи як виклики безпеці ЄС: історія розвитку та сьогодення. *Право та інновації.* 2023. № 1 (41). С. 96–104.
2. Бойчук Д. С. Право людини на захист: загальнотеоретична характеристика: дис. на здобуття наук. ступеня канд. наук :Харків, 2018.
3. Бойчук, Д. С. Щодо питання про право на зброю як складову частину права людини на захист. *Правові новели* № 4. 2018. 9–14.
4. Yakoviyk, I. V., Tragniuk, O. Y., & Boichuk, D. S. Strategic Autonomy of the European Union: On the Way to" European Sovereignty" in Defense?. *Probs. Legality*, *149*, 2020. 223.
5. Kamile Nur Seviş, Ensar Seker. Cyber Warfare: Terms, Issues, Laws and Controversies.URL: https://www.researchgate.net/publication/306064145_Cyber_warfare_terms_issues_laws_and_controversies. (дата звернення: 10.12.2023).
6. National Cyber Security Strategies: An Implementation Guide. The European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide. (дата звернення: 10.12.2023).
7. Даніленкова І.М. Проблеми розвитку та функціонування інститутів спільного інвестування в Україні. Стратегічні орієнтири. URL: http://libfor.com/index.php?newsid=32 (дата звернення: 10.12.2023).
8. Сопілко І. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник*. 2021. № 59. С. 110–115. URL: https://dspace.nau.edu.ua/bitstream/NAU/53733/1/I.%20M.%20Сопілко.pdf.(дата звернення: 10.12.2023).
9. Діордіца І. Поняття та зміст національної системи кібербезпеки. *National law journal: teory and practice*.2016.С. 33–38. URL: https://ibn.idsi.md/sites/default/files/imag_file/33_38_Ponyattya%20ta%20zmIst%20natsIonalnoYi%20sistemi%20kIberbezpeki.pdf. (дата звернення: 10.12.2023).
10. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.
11. Баранов О. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика.* 2014. Т. 42, № 2. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf (дата звернення: 10.12.2023).
12. Giantas D., N. Liaropoulos A. Cybersecurity in the EU: Threats, Frameworks and future perspectives. 2019. 40 p.
13. Pascale Davies. Estonia hit by 'most extensive' cyberattack since 2007 amid tensions with Russia over Ukraine war. URL: https://www.euronews.com/next/2022/08/18/estonia-hit-by-most-extensive-cyberattack-since-2007-amid-tensions-with-russia-over-ukrain. (дата звернення: 11.12.2023).
14. Kertu Ruus. Cyber War I: Estonia Attacked from Russia. *European Affairs A publication of: The European Institute*. 2008. № 9. URL: https://ciaotest.cc.columbia.edu/journals/ea/v9i1/03.html. (дата звернення: 11.12.2023).
15. National Plan for Information Infractructure Protection. URL: https://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf. (дата звернення: 11.12.2023).
16. Strategy to improve Internet security in Sweden. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Sweden_2006_Strategy_Internet_security_2006_12_July_2006.pdf. (дата звернення: 11.12.2023).
17. Ministry of Defence. Cyber Security Strategy. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en. (дата звернення: 11.12.2023).
18. Finland´s cyber security strategy. *Government Resolution*. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf. (дата звернення: 11.12.2023).
19. Myriam Dunn, Center for Security Studies, Swiss Federal Institute of Technology (ETH Zurich). A comparative analysis of cybersecurity initiatives worldwide. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf. (дата звернення: 11.12.2023).
20. National Strategy for Information Security in the Slovak Republic. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Slovakia_National_Strategy_for_ISEC.pdf. (дата звернення: 11.12.2023).
21. French national digital security strategy. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf. (дата звернення: 11.12.2023)
22. Cyberspace protection policy of the republic of poland. *Republic of poland ministry of administration and digitisation, internal security agency*. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf. (дата звернення: 13.12.2023).

23. National cyber security strategies. *National cyber security strategies*. URL: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf. (дата звернення: 13.12.2023).
24. Hungary's national security strategy. URL: https://eda.europa.eu/docs/default-source/documents/hungary-national-security-strategy-2012.pdf. (дата звернення: 13.12.2023).
25. Cyber security and politically, socially and religiously motivated cyber attacks. *Directorate-general for external policies of the union directorate b – policy department* -. URL: https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf. (дата звернення: 13.12.2023).
26. Садомська Б. Український кіберпростір: безпекові загрози, виклики та перспективи розвитку. *Аналітичний центр ADASTRA*. 2020. URL:: https://adastra.org.ua/blog/ukrayinskij-kiberprostir-bezpekovi-zagrozi-vikliki-ta-perspektivi-rozvitku. (дата звернення: 13.12.2023).
27. Norway blames Russia for cyber-attack on parliament. *BBC*. 2020. URL: https://www.bbc.com/news/world-europe-54518106. (дата звернення: 13.12.2023).
28. Paganini P. Denmark blamed russia apt28 group for cyber intrusions in defense ministry emails. *Danish Defense Ministry.* 2017. URL: https://securityaffairs.com/58322/hacking/apt28-hacked-denmark-defense-ministry.html. (дата звернення: 13.12.2023).
29. Dutch intelligence: Many cyberattacks by Russia are not yet public knowledge. *The Record*. URL: https://therecord.media/dutch-intelligence-russia-cyberattacks-many-not-yet-public-knowledge. (дата звернення: 13.12.2023).
30. Paganini P. Russia suspected over cyber espionage campaign on the italian foreign ministry. *Danish Defense Ministry.* 2017. URL: https://securityaffairs.com/56157/intelligence/italian-foreign-ministry-hacked.html. (дата звернення: 13.12.2023).
31. Enisa threat landscape. European Union Agency for Cybersecurity (ENISA). 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. (дата звернення: 13.12.2023).
32. European Cybersecurity Index: European Countries with the Best and Worst Cybersecurity 2021. URL: https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/. (дата звернення: 13.12.2023).
33. ENISA Threat Landscape 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. (дата звернення: 13.12.2023).
34. Directive (EU) 2016/1148 of the European Parliament and of the Council. 2016. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. (дата звернення: 13.12.2023).
35. European Security Union 2020-2025. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en. (дата звернення: 13.12.2023).
36. Judgment of the Court (Grand Chamber) of 8 June 2010 Case C-58/08. The Queen, on the application of: Vodafone Ltd and Others. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0058. (дата звернення: 13.12.2023).
37. Proposal for a directive of the european parliament and of the council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN. (дата звернення: 13.12.2023).
38. Treaty establishing the European Community. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12002E%2FTXT. (дата звернення: 13.12.2023)
39. Penalties for NIS2 Violations. URL: https://nis2directive.eu/nis2-fines/. (дата звернення: 13.12.2023).