ПРЯМУЄМО РАЗОМ

ВЕРХОВНА РАДА УКРАЇНИ

UNDP

Проєкт ЄС-ПРООН з парламентської реформи

Комітет з питань цифрової трансформації

АНАЛІТИЧНИЙ ЗВІТ

Норми законодавства Європейського Союзу, які необхідно впровадити в проєкти законів про кібербезпеку та про об'єкти критичної інфраструктури в Україні

Публікація підготовлена в рамках проєкту ЄС-ПРООН з парламентської реформи. Зміст публікації є виключно відповідальністю автора і необов'язково відображає позицію Європейського Союзу або Програми розвитку ООН.

Авторка — **Лілія Олексюк**, кандидат наук з державного управління, юрист, позаштатний консультант Комітету Верховної Ради України з питань цифрової трансформації.

ЗМІСТ

СКОРОЧЕННЯ

CERT	комп'ютерні групи реагування на надзвичайні ситуації
CSIRT	група з реагування на інциденти в галузі комп'ютерної безпеки
ENISA	Агентство Європейського Союзу з питань мережевої та інформаційної безпеки
GDPR	Загальний регламент захисту даних
LEA	law enforcement agency, правоохоронний орган
Адміністративні домовленості	Адміністративні домовленості щодо охорони інформації з обмеженим доступом між урядом України та Організацією Північноатлантичного договору, ратифіковані Законом №2068-VIII від 24.05.2017 р.
Директива 114	Директива Ради 2008/114/ЄС від 8 грудня 2008 р. про ідентифікацію та призначення європейських критичних інфраструктур та оцінку необхідності вдосконалення їх захисту
Директива NIS	Директива з безпеки мережевих та інформаційних систем
ЄК	Європейська Комісія
ЄКІ	європейська критична інфраструктура
ЄС	Європейський Союз
ЄЦР ЄС	Єдиний цифровий ринок ЄС
ІКТ	інформаційно-комунікаційні технології

Комітет з питань цифрової трансформації	Комітет Верховної Ради України з питань цифрової трансформації
НАТО	Організація Північноатлантичного договору
ОКІ	об'єкти критичної інфраструктури
ООП	оператори основних послуг
Регламент 1807	Регламент (ЄС) 2018/1807 Європейського Парламенту та Ради від 14 листопада 2018 р. про рамки для вільного обміну неособистими даними в Європейському Союзі
РНБО	Рада національної безпеки та оборони
Угода про асоціацію	Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони
Угода з НАТО	Угода про безпеку між Урядом України і Організацією Північноатлантичного договору, ратифікована Законом №160-IV від 12.09.2002 р.

РЕЗЮМЕ

Україна перебуває на початковому етапі імплементації до українського законодавства актів законодавства Європейського Союзу (далі — ЄС) в частині кібербезпеки та захисту об'єктів критичної інфраструктури.

Законодавство щодо державного регулювання в зазначених сферах без огляду на строк його застосування потребує суттєвого доопрацювання і корекції з огляду на необхідність тіснішої співпраці і взаємодії із ЄС та НАТО, а в частині захисту об'єктів критичної інфраструктури — розробки повноцінної державної політики (законодавчої бази, організаційних, економічних та фінансових заходів).

Узгодження терміносистем, процедур і протоколів взаємодії між Україною та ЄС може посилити загальну спільну безпеку кіберпростору.

Відповідно до Національного індексу кібербезпеки, за яким Естонська академія електронного врядування вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами, Україна посідає в рейтингу 28 місце з-поміж 152 країн[1].

Аналіз складових Національного індексу кібербезпеки показує повну відсутність заходів, застарілість чи нечинність певної інформації. Рейтинг складався на підставі офіційних даних органів влади, але їхня оцінка відрізняється від оцінки, наданої громадянським суспільством і експертами в цій сфері[2,3].

1 https://ncsi.ega.ee/ncsi-index/

2 https://www.pravda.com.ua/columns/2019/09/14/7226291/

3 https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

На підставі Національного індексу кібербезпеки слід зазначити, що в Україні зафіксовано повну відсутність деяких складових кібербезпеки:

- відсутній підрозділ аналізу кіберзагроз;
- відсутні опубліковані щорічні громадські звіти; відсутні вимоги до компетенцій з кібербезпеки у молодшій та середній школі;
- країна не входить до регіональної чи міжнародної організації з кібербезпеки;
- за останні 3 роки країна не (спів)фінансувала або (спільно) не організувала принаймні один проєкт з нарощування потенціалу для іншої країни;
- відсутній стандарт кібербезпеки для державного сектора; уряд не має компетентного органа в галузі кібер/інформаційної безпеки, уповноваженого контролювати державних та приватних постачальників цифрових послуг щодо виконання вимог кібер/інформаційної безпеки;
- відсутній регулярний моніторинг заходів кібербезпеки;
- не встановлено регулювання для відмітки часу при наданні електронних довірчих послуг;
- уряд не призначив єдину контактну точку для міжнародної координації кібербезпеки;
- відсутні механізми врегулювання кіберкриз[4];
- відсутній підрозділ із військових кібероперацій (не призначений відповідно до українського законодавства); не впроваджено відповідне тренування з моделюванням сценаріїв інцидентів у реальному часі, яке має важливе значення для перевірки готовності й співпраці держав-членів у питаннях безпеки мережевих та інформаційних систем.

Згідно з дослідженнями науковців[5], індекс розвитку цифрової економіки DESI[6] для України становить 0,18, що значно нижче за середнє значення в ЄС.

З метою розвитку цифрової економіки та забезпечення національної безпеки в кіберпросторі необхідно здійснити низку узгоджених із ЄС дій, які можуть слугувати базою для Єдиного цифрового ринку[7] між Україною і ЄС.

У Спільній декларації саміту Східного партнерства (далі — СхП) у листопаді 2017 року учасники саміту погодилися співпрацювати у сфері гармонізації цифрових ринків, щоб поширити вигоди ЄЦР ЄС для країн-партнерів[8]. Відповідний пріоритет (№7) зазначений серед 20 очікуваних досягнень СхП до 2020 року[9].

---

4 https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

5 http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nzundiz_2015_5_3.pdf

6 https://ec.europa.eu/digital-single-market/en/desi

7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0192

8 https://www.consilium.europa.eu/media/31758/final-statement-st14821en17.pdf

9 https://cdn3-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/dLJ9RdBalFgQqx34lgPlwagsNIuJB6cJzDeeiRR0RdQ/mtime:1497363650/sites/eeas/files/swd_2017_300_f1_joint_staff_working_paper_en_v5_p1_940530.pdf

ВСТУП

Створення та впровадження ефективної й результативної національної системи кіберзахисту визначено одним із пріоритетів державної політики у сфері національної безпеки України; ці процеси динамічно розгортаються й спрямовані на адекватне та випереджальне реагування на дедалі більші виклики та загрози в національному й міжнародному кіберпросторі.

Розбудова національної системи кіберзахисту триває від створення незалежної держави Україна, хоча слова «кібербезпека» чи «кібертероризм» з'явилися набагато пізніше. До 2006 року, в Законі України «Про основи національної безпеки» в редакції 2003 року, загрозами національним інтересам і національній безпеці України в інформаційній сфері названо комп'ютерні злочини та комп'ютерний тероризм[10].

«Проблемам забезпечення безпеки інформації, захисту інформаційного простору України від небажаного інформаційного впливу, забезпечення безпечного функціонування ІТС та захисту інформації, що циркулює в них, приділялась серйозна увага з перших днів існування української держави. Вже наступного дня після проголошення Декларації про незалежність України — 25 серпня 1991 року — було ухвалено рішення щодо прийняття під юрисдикцію держави спеціальних видів зв'язку, а прийнятим у березні 1992 року Законом України «Про Службу безпеки України» законодавчо визначено порядок забезпечення засекреченим і шифрованим документальним зв'язком державних органів та відповідальних посадових осіб»[11].

Сучасний етап розбудови національної системи кіберзахисту розпочався у 2006 році, коли Україна приєдналася до Конвенції про кіберзлочинність і визнала «необхідність співробітництва між Державами і приватними підприємствами для боротьби з кіберзлочинністю і необхідність захисту законних інтересів у ході використання і розвитку інформаційних технологій»[12].

10 https://zakon.rada.gov.ua/laws/show/964-15/ed20030619

11 http://ela.kpi.ua/bitstream/123456789/12522/1/05_p7.pdf

12 http:// http://www.niss.gov.ua/sites/default/files/2019-02/Analit_Dopovid_Poslannia_2018.pdf

Для імплементації цієї Конвенції необхідно було розробити механізми співпраці держави й приватного сектору в частині забезпечення кібербезпеки, при цьому зберігаючи «належний баланс між правоохоронними інтересами і повагою до основних прав людини»[13], переглянути законодавство України в частині процедурних питань задля забезпечення можливості отримання належних доказів у кримінальних справах із використанням інформаційно-телекомунікаційних мереж і технологій, формулювання самого складу злочину у цифровому світі, забезпечити спеціалістів як для професійного розслідування кримінальних проваджень, так і для адекватного розгляду справ у судах — фахівців, які зможуть встановити факти і забезпечити невідворотність покарання за ці види злочинів.

Паралельно із розвитком внутрішньої інформаційної політики України увага приділялася й вектору зовнішньої політики, а саме — удосконаленню законодавства у сфері забезпечення кібербезпеки, розбудови системи кіберзахисту й імплементації законодавства ЄС у національне; ці процеси активізувалися із підготовкою, а потім і підписанням Угоди про асоціацію з ЄС.

Ратифікація Верховною Радою України та Європейським Парламентом Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони[14] (далі — Угода про асоціацію), відкрила перед Україною потенційні можливості впровадження європейських стандартів та інтеграції до Єдиного цифрового ринку ЄС.

Водночас ЄС у 2015 році розпочав реалізацію Стратегії створення єдиного цифрового ринку ЄС. Цифровізація економіки має визначати конкурентні позиції держав у наступні роки, оскільки цифрова революція відбувається швидшими темпами, ніж колись індустріальні революції.

Єдиний цифровий ринок — це задекларована Європейською Комісією (ЄК) у травні 2015 року стратегія, яка охоплює Єдиний європейський ринок, пов'язана зі сферами електронної комерції та телекомунікацій, але за умови безпеки: даних, споживачів та переміщення товарів і послуг.

За визначенням Європейської Комісії, єдиний цифровий ринок ЄС — такий, у якому забезпечено вільне переміщення товарів, осіб, послуг і капіталу, у межах якого окремі особи та підприємства можуть безперешкодно отримувати доступ і здійснювати електронну діяльність в умовах конкуренції, де забезпечено високий рівень захисту прав споживачів, незалежно від їхнього громадянства чи місця проживання, і їхніх персональних даних. Досягнення єдиного цифрового ринку, на думку ЄК, забезпечить Європейському Союзу збереження позиції світового лідера у сфері цифрової економіки, допоможе європейським компаніям зростати глобально.

ЄС має бажання очолити глобальну цифрову економіку. Фрагментарність і бар'єри, наявні зараз на цифрових ринках країн ЄС, гальмують процеси розвитку економіки. Знищення цих бар'єрів може принести додаткові 415 млрд євро до ВВП ЄС.

13 https://zakon.rada.gov.ua/laws/show/994_575

14 https://zakon.rada.gov.ua/laws/show/984_011

Цифрова економіка може розширювати ринки та стимулювати удосконалені е-послуги за вигіднішими цінами, пропонувати широкий вибір і створювати нові джерела зайнятості та нову додану вартість. Єдиний цифровий ринок забезпечує нові можливості для компаній, стартапів і дає змогу бізнесам зростати й отримувати прибутки від масштабованого сегменту обсягом у понад 500 млн осіб.

У стратегію Єдиного цифрового ринку ЄС[15] закладено три основні напрями:

1) покращення споживачам і бізнесу доступу до товарів і послуг у глобальній мережі інтернет по всій Європі, що вимагає швидкого усунення основних відмінностей між онлайновими та офлайновими просторами для подолання бар'єрів у транскордонній електронній діяльності;

2) створення належних умов для просування інфокомунікаційних мереж і послуг, для чого потрібні високошвидкісні та надійні інфраструктура й послуги зі створення контенту, підтримувані нормативними актами, що забезпечують інновації, інвестиції, конкуренцію та рівність умов;

3) максимізація потенціалу зростання цифрової економіки ЄС, що вимагає інвестицій до інфраструктури та ІКТ, зокрема хмарних обчислень та великих даних, а також досліджень та інновацій, спрямованих на підвищення конкурентоспроможності промисловості, покращення державних послуг, формування цифрових навичок.

Ключовими завданнями в рамках наближення законодавства України до законодавства ЄС задля поширення режиму внутрішнього ринку ЄС на базову для цифрової економіки сферу телекомунікацій (електронних комунікацій) є імплементація актів ЄС у законодавство України.

Інтеграція України до Єдиного цифрового ринку ЄС є одним із найпріоритетніших завдань для України. Угода про асоціацію між Україною та ЄС закладає чітке юридичне підґрунтя для досягнення цієї мети (статті 115–124, 139, 140, 389–395, 463, 2–6 Додатку XVII).

Угода про асоціацію передбачає перспективу взаємного надання режиму внутрішнього ринку в секторі телекомунікаційних послуг. Відповідно до статті 4(3) Додатку XVII до Угоди про асоціацію, такий режим означає, що в цьому секторі не має бути обмежень щодо надання послуг українською юридичною особою на території ЄС і навпаки. Режим можна отримати за умови позитивного оцінювання Європейським Союзом кроків України з наближення нормативно-правових актів України до права ЄС.

Зближення ринків можливе за умови:

1) наближення нормативно-правового регулювання;

2) наявності тотожних регуляторів ринку та чіткого розподілу повноважень між органами, якщо регуляторів сфери, що належить до певного ринку, більш ніж один;

3) однакового або зрозумілого технічного регулювання й стандартизації сфери.

15 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN

Таким чином, інтеграція України до Єдиного цифрового ринку ЄС можлива за умови наближення усіх трьох складових до європейських норм, правил і стандартів.

У рамках виконання завдань забезпечення кібербезпеки України та створення можливостей для участі в Єдиному цифровому ринку ЄС Верховна Рада України ухвалила Закон України «Про основні засади забезпечення кібербезпеки України» (набув чинності з 9 травня 2018 року), яким, зокрема, визначено сферу застосування закону, понятійний апарат, базові принципи, об'єкти та суб'єкти кібербезпеки й кіберзахисту, їхні завдання, способи державно-приватного партнерства, у тому числі й щодо формування і розвитку системи кіберзахисту об'єктів критичної інфраструктури.

На підставі зазначеного закону суб'єкти кібербезпеки та кіберзахиситу розробили низку підзаконних актів, якими затверджено порядок формування переліку об'єктів критичної інформаційної інфраструктури, порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування; загальні вимоги щодо кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури; критерії формування переліку об'єктів критично інформаційної інфраструктури. Але більшість із них досі залишаються у статусі проєктів.

З огляду на важливість та актуальність завдань щодо захисту об'єктів критичної інфраструктури, зокрема критичної інформаційної інфраструктури, уряд ухвалив Концепцію створення державної системи захисту критичної інфраструктури[16], якою визначено шляхи і способи розв'язання проблем забезпечення захисту критичної інфраструктури. Серед них — розробка проєкту Закону України «Про критичну інфраструктуру та її захист», яким має бути визначено основні напрями, принципи, механізми й строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління у сфері захисту критичної інфраструктури, комплекс заходів на загальнодержавному, регіональному, галузевому, а також на місцевому та об'єктовому рівнях, критерії, за сукупністю яких об'єкти мають відноситися до критичної інфраструктури, порядок категоризації та паспортизації таких об'єктів, складання та ведення їх реєстру, а також завдання з кіберзахисту суб'єктів державної системи захисту критичної інфраструктури та загальні вимоги з кіберзахисту до операторів критичної інфраструктури.

Цей аналітичний звіт містить огляд основних документів, які Україна має намір імплементувати в законодавство відповідно до зобов'язань, взятих на себе під час підписання Угоди про асоціацію, та з метою «реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору»[17], а також відповідно до нових домовленостей, схвалених Радою асоціації України та ЄС.

16 https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80

17 https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

ЕТАПИ ІМПЛЕМЕНТАЦІЇ

Угодою про асоціацію прямо не передбачено зобов'язань щодо імплементації актів ЄС з кібербезпеки та захисту об'єктів критичної інфраструктури. Але оскільки вони є фундаментальними засадами Єдиного цифрового ринку ЄС, а Україна має на меті приєднатися до нього, постала необхідність визначити механізми й процедури імплементації актів, що не увійшли до числа Додатків до Угоди про асоціацію.

У грудні 2019 року було оновлено План заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затверджений Постановою Кабінету Міністрів України №1106 від 25 жовтня 2017 р. «Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони» (зі змінами) (далі — План заходів).

Цей План заходів містив такі завдання та акти ЄС, які Україна має намір виконати шляхом імплементації (*див. Таблицю 1*).

Таблиця 1. Завдання щодо імплементації Угоди про асоціацію в частині кібербезпеки[18]

Найменування завдання	Положення / рішення	Акт права ЄС	Найменування заходу	Строк виконання	Відповідальні за виконання
19391. Забезпечення високого загального рівня безпеки мережевих та інформаційних систем	Статті 391, 394	· Директива (ЄС) 2016/1148; · Імплементаційний Регламент Комісії (ЄС) 2018/151; · Імплементаційне Рішення Комісії (ЄС) 2017/179	1) Приведення у відповідність із правом ЄС термінології у сфері безпеки мережевих та інформаційних систем; 2) законодавче закріплення вимог щодо критеріїв ідентифікації операторів основних послуг;	До 31 грудня 2023 р.	· Адміністрація Держспецзв'язку; · Мінцифри; · НКРЗІ (за згодою); · МВС; · СБУ (за згодою)

18 https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF

			3) забезпечення компетентних органів на законодавчому рівні необхідними повноваженнями та ресурсами для проведення оцінки виконання операторами основних послуг своїх зобов'язань; 4) встановлення на законодавчому рівні повноважень для компетентних органів за необхідності вживати наглядових заходів для подальшого реагування у разі отримання доказів щодо невиконання провайдером цифрових послуг установлених вимог		
19394. Налагодження співробітництва з Агенцією ЄС з питань мережевої та інформаційної безпеки	Стаття 394	· Регламент (ЄС) 526/2013	Підписання двосторонньої угоди з Агенцією ЄС з питань мережевої та інформаційної безпеки	До 31 грудня	· Адміністрація Держспецзв'язку; · Мінцифри; · НКРЗІ (за згодою); · МВС; · СБУ (за згодою)
193912. Законодавче забезпечення вільного руху неперсональних даних	Статті 391, 394	· Регламент (ЄС) 2018/1807	Встановлення вимог щодо локалізації даних, наявності даних для компетентних органів і передачі даних для професійних користувачів	До грудня 2023 р.	· Мінцифри

У квітні 2018 року Україна надала для розгляду ЄС звернення (Non Paper) про розширення сфери дії Угоди про асоціацію та оновлення Додатку XVII до Угоди про асоціацію — внесення до нього 18 актів законодавства ЄС. Документ було проаналізовано місією ЄС[19], оскільки більшість цих матеріалів також були перелічені в Плані заходів[20], що теж подавався для аналізу.

Більшість із законодавчих актів, перелічених у документі, безпосередньо не стосуються телекомунікаційних послуг. Через специфічні положення Додатку про телекомунікації включення цих актів розширило б саме сферу телекомунікацій, хоча ці акти є лише дотичними і формально до цієї царини не належать. При цьому деякі інші сфери, що підлягають імплементації (електронна торгівля, захист прав споживачів тощо), зазначені в інших розділах чи додатках Угоди про асоціацію.

19 https://www.rbc.ua/ukr/news/ukraine-nachala-rabotu-otsenochnaya-missiya-1566040528.html

20 https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF

Влітку 2018 року в контексті обговорень запиту ЄС повідомив Україні, що неофіційний документ не є достатньою основою для подальшої співпраці, адже Угода про асоціацію чітко передбачає формальні підстави для співробітництва в галузях, на які поширюється Додаток XVII. Таким формальним кроком є подання дорожньої карти, вимоги до якої викладені у статті 2 Додатку XVII-6 до Угоди про асоціацію[21].

У серпні 2018 року Україна подала Цифрову дорожню карту, розроблену на підставі Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та плану заходів щодо її реалізації[22], де окреслено заходи з імплементації правових актів, що містяться в Додатку про телекомунікації. Крім того, ця дорожня карта також містить заходи з впровадження ширшого переліку нормативно-правових актів, зокрема попередніх, поданих у квітні 2018 року.

З огляду на важливість цього документу та визначені юридичні питання ЄК запропонувала багатоетапний процес оцінки цифрової дорожньої карти.

У межах виконання наявних зобов'язань передбачено три фази процесу:

- **Фаза 1:** внутрішній глибокий аналіз кожного акта, зазначеного в Дорожній карті.
- **Фаза 2:** оцінка виконання наявних зобов'язань, адміністративної спроможності та законодавства на практиці (зокрема оцінка на місці).
- **Фаза 3:** робочий план виконання зобов'язань відповідно до Додатку XVII до Угоди про асоціацію із зазначенням пріоритетів, термінів та орієнтирів виконання.

Європейська Комісія запропонувала цей багатоступеневий процес, прагнучи надати Україні конструктивну та прагматичну допомогу у виконанні зобов'язань за Угодою про асоціацію. При цьому багатоетапний процес не замінює інші формальні кроки, передбачені в Угоді про асоціацію.

Режим внутрішнього ринку у секторі не надається автоматично. Щойно Україна переконається, що умови фази завершення, прийняття та впровадження, зокрема забезпечення належного регуляторного потенціалу та нагляду в певному секторі, а також усі домовленості виконано, вона має повідомити ЄС про необхідність комплексної оцінки в цьому секторі. Тільки після успішного проходження оцінки ЄС та Україна можуть вирішити надати одне одному режим внутрішнього ринку в секторі.

Наразі Україна за результатами перемовин із ЄС узгодила інший механізм внесення змін до Угоди та оновлення додатків[23], який стане в пригоді для вирішення питання імплементації актів ЄС, що не увійшли до Угоди про асоціацію або були змінені з часу її підписання.

21 https://zakon.rada.gov.ua/laws/show/984_011

22 https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80

23 http://reforms.in.ua/sites/default/files/field/files/docs/ac_council_dec_1-2019.pdf

ЗАКОНОДАВСТВО ЄС ТА ПОТОЧНИЙ СТАН ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ

У Європейському Союзі під мережевою та інформаційною безпекою розуміють здатність мережі чи інформаційної системи протистояти суперечливим випадковим подіям або незаконним чи зловмисним діям, що несуть загрозу для доступності, автентичності, цілісності та конфіденційності збережених або переданих даних і відповідних послуг, пропонованих або доступних через ці мережі та системи.

Для організації взаємодії країн ЄС у питаннях забезпечення безпеки спеціально створене Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA). Також ENISA має аналізувати стратегії мережевої та інформаційної безпеки, сприяти представленню їх у форматі, що надається до порівняння, забезпечувати за допомогою електронних засобів доступність для громадськості стратегій та результатів їх аналізу, оприлюднених інституцією, органом, офісом або агентством Союзу чи державою-членом і наданих ENISA для отримання інформації та уникнення дублювання.

Директива з безпеки мережевих та інформаційних систем (Директива NIS) становить першу частину законодавства ЄС щодо кібербезпеки. Вона забезпечує правові заходи, спрямовані на підвищення загального рівня кібербезпеки в ЄС. Документ ухвалений Європейським Парламентом 6 липня 2016 року і набрав чинності в серпні 2016 року, але держави-члени мали 21 місяць, щоб транспонувати Директиву до своїх національних законів і понад 6 місяців, щоб визначити операторів основних послуг.

Директива NIS передбачає юридичні заходи для підвищення загального рівня кібербезпеки в ЄС. Для цього вона вимагає забезпечити:

- готовність держав-членів, їхнє належне оснащення, наприклад наявність групи з реагування на інциденти в галузі комп'ютерної безпеки (CSIRT) та компетентного національного органа (або органів);

- співробітництво між усіма державами-членами шляхом створення групи співпраці з метою підтримки та сприяння стратегічній взаємодії та обміну інформацією між державами-членами. Крім того, їм необхідно буде встановити мережу CSIRT, щоб сприяти швидкому та ефективному оперативному співробітництву щодо конкретних випадків кібербезпеки та обміну інформацією про ризики;
- культуру безпеки між секторами, що є життєво важливими для економіки та суспільства і, крім того, сильно залежать від ІКТ, наприклад: енергетика, транспорт, водопостачання, банківська справа, інфраструктура фінансового ринку, охорона здоров'я та цифрова інфраструктура. Підприємства в цих секторах, що визначені державами-членами як оператори основних послуг, мають вживати відповідних заходів безпеки та повідомляти відповідним національним органам про серйозні інциденти. Крім того, основні цифрові постачальники послуг (пошукові системи, служби хмарних обчислень та інтернет-магазини) повинні відповідати вимогам безпеки та інформування відповідно до нової Директиви.

Сьомий пріоритет Східного партнерства до 2020 року «Зосередження уваги на ключових пріоритетах та відчутних результатах»[24] також підтверджує необхідність узгодження безпекових стратегій для досягнення єдиного цифрового ринку як в ЄС, так і з третіми країнами.

7 червня 2019 року в Офіційному журналі ЄС опубліковано Регламент про кібербезпеку Європейського Союзу (Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з питань кібербезпеки) та про сертифікацію кібербезпеки в галузі інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) №526/2013) (далі — Регламент про кібербезпеку). Документ набрав чинності 27 червня 2019 року.

Законодавство ЄС має на меті зміцнити спроможність Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) допомагати державам-членам подолати загрози кібербезпеки.

Законодавство ЄС про кібербезпеку має дві основні цілі:

1) посилення мандата ENISA як наглядового органа ЄС у царині кібербезпеки, задля підтримки держав-членів ЄС у подоланні загроз та атак у цій сфері;
2 створення загальноєвропейської системи сертифікації кібербезпеки (Рамки), в якій ENISA відіграватиме ключову роль.

Відповідно до Регламент про кібербезпеку ENISA має координувати підготовку запропонованих схем сертифікації кібербезпеки, що подаються для ухвалення до Європейської Комісії. Регламент дасть можливість видавати європейські сертифікати кібербезпеки та акти про відповідність продукції, послуг та процесів ІКТ у всіх країнах-членах ЄС.

24 https://www.eurointegration.com.ua/articles/2017/11/24/7074139/

Законодавство про кібербезпеку пропонує бізнесам можливість засвідчити, що їхня продукція відповідає стандартам кібербезпеки ЄС. Сертифікація з питань кібербезпеки буде добровільною, якщо інше не встановлено законодавством ЄС або країн-членів. Комісія ЄС регулярно оцінюватиме необхідність впровадження обов'язкових сертифікацій.

Схема сертифікації може визначати один або кілька рівнів забезпечення безпеки: базовий, значний або високий. На базовому рівні виробники ІКТ або постачальники послуг зможуть самі здійснювати оцінку відповідності. У випадку значного чи високого рівня оцінювання здійснюватимуть національні органи з сертифікації кібербезпеки.

Держави-члени ЄС мали розробити законодавчі норми щодо відповідальності за порушення вимог Регламенту та за порушення схем сертифікації кібербезпеки ЄС.

Законодавство про кібербезпеку є частиною загальної кіберекосистеми Європейського Союзу, мета якої — підвищення безпеки цифрового середовища Європейського Союзу та безпечне використання інформаційних послуг на Єдиному цифровому ринку.

Екосистема кібербезпеки, відповідно до стандарту ETSI TR 103 306 V1.4.1 (2020-03), складається з постійного циклу структурованих дій:

- визначити (зрозуміти стан та ризики для систем, активів, даних і можливостей);
- захистити (впровадити відповідні гарантії);
- виявити (реалізувати здатність ідентифікувати кібербезпеку);
- відреагувати (реалізувати здатність вживати заходів у відповідь на загрозу кібербезпеці);
- відновлювати (забезпечити стійкість і відновлення порушених можливостей).

Цей самий стандарт визначає кібербезпеку як «сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, настанов, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій та технологій, які можна використовувати для захисту кіберсередовища і організації та активів користувача»[25].

Таким чином, до законодавства ЄС, яке необхідно імплементувати, належать такі документи (перелік не вичерпний):

1. Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива NIS)[26], що встановлює вимоги щодо сповіщення та безпеки для операторів основних послуг та постачальників цифрових, наприклад хмарних, послуг.

25 https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.04.01_60/tr_103306v010401p.pdf

26 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

2 Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент захисту даних, далі — GDPR)[27].

3 Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або притягнення до відповідальності за кримінальні злочини чи виконання кримінальних покарань, а також про вільний рух таких даних та скасування Рамкового рішення Ради 2008/977/ПВР[28] (далі — Директива 680);

4 Директива 2002/58/ЄС Європейського Парламенту та Ради від 12 липня 2002 року щодо обробки персональних даних та захисту конфіденційності в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації)[29] і розроблений на її заміну Проєкт Регламенту електронної конфіденційності, спрямований на захист прав на приватність та конфіденційність комунікацій, а також на просування надійного та безпечного «Інтернету речей» на єдиному цифровому ринку[30].

5 Директива 2014/24/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року щодо державних закупівель та скасування Директиви 2004/18/ЄС[31].

6 Регламент (ЄС) №593/2008 Європейського Парламенту та Ради від 17 червня 2008 року «Про право, що застосовується до договірних зобов'язань (Рим I)»[32].

7 Директива (ЄС) 2015/1535 Європейського Парламенту та Ради від 9 вересня 2015 року, що встановлює порядок надання інформації у сфері технічних регламентів та правил щодо послуг інформаційного суспільства[33].

8 Рамкове рішення Ради 2006/960/JHA від 18 грудня 2006 року «Про спрощення обміну інформацією та розвідувальних данних між правоохоронними органами держав-членів Європейського Союзу»[34].

9 Директива 2014/41/ЄС Європейського Парламенту та Ради від 3 квітня 2014 року щодо Європейського наказу про розслідування у кримінальних справах[35].

10 Конвенція Ради Європи про кіберзлочинність, CETS №185[36].

27 https://eur-lex.europa.eu/eli/reg/2016/679/oj
28 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680
29 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
30 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010#footnote23
31 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024
32 https://zakon.rada.gov.ua/go/994_905
33 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L1535&from=BG
34 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006F0960
35 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041
36 https://zakon.rada.gov.ua/go/994_575

11 Регламент Ради (ЄС) №1206/2001 від 28 травня 2001 року про співпрацю між судами держав-членів у справі отримання доказів у цивільних чи господарських справах[37].

12 Директива 2008/114/ЄС від 8 грудня 2008 року Європейського Парламенту та Ради про ідентифікацію та призначення європейських критичних інфраструктур та оцінку необхідності вдосконалення їх захисту[38].

13 Регламент (ЄС) 2018/1807 Європейського Парламенту та Ради від 14 листопада 2018 р. про рамки для вільного обміну неособистими даними в Європейському Союзі[39].

Законодавство Європейського Союзу про кібербезпеку не розглядає окремо заходи з кібербезпеки, захист конфіденційності й захист мереж та / або інформаційних систем, а має на меті узгоджені дії щодо захисту засобів, інформації та конфіденційності як частину екосистеми кібербезпеки.

Директива NIS є першим інструментом внутрішнього ринку, спрямованим на підвищення опірності ЄС до ризиків у сфері кібербезпеки. Вона орієнтована на забезпечення безперервності послуг, що дають економіці та суспільству ЄС змогу функціонувати належним чином. З цією метою Директива NIS запроваджує конкретні заходи з розбудови можливостей кібербезпеки в ЄС та зменшення зростаючих загроз для мережевих та інформаційних систем, які використовуються для надання основних послуг у ключових секторах.

Директива NIS:

«(a) встановлює обов'язки всіх держав-членів щодо **ухвалення національної стратегії з безпеки мережевих та інформаційних систем**;

(b) створює **Групу з питань співробітництва** з метою підтримки та сприяння стратегічному співробітництву й обміну інформацією між державами-членами та розвитку довіри між ними;

(c) створює **мережу команд реагування на комп'ютерну безпеку** («мережа CSIRT»), щоб сприяти розвитку довіри між державами-членами й швидкій та ефективній оперативній співпраці;

(г) встановлює **вимоги щодо безпеки та оповіщення для операторів основних послуг та для постачальників цифрових послуг**;

(e) встановлює **обов'язки держав-членів щодо призначення національних компетентних органів, єдиних контактних пунктів та CSIRT із завданнями, пов'язаними з безпекою мережевих та інформаційних систем**»[40].

37 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001R1206

38 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114

39 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807#ntr3-L_2018303EN.01005901-E0003

40 https://eur-lex.europa.eu/eli/reg/2019/881/oj

Після набрання Директивою NIS чинності, тобто з серпня 2016 року, держави-члени мали до 9 травня 2018 року імплементувати у національне законодавство інструменти й заходи, необхідні для виконання положень Директиви.

У додатку II до Директиви NIS вміщено перелік секторів, відповідних галузей та типів суб'єктів, які мають значення для процесу ідентифікації операторів основних послуг (ООП) (*див. Таблицю 2*).

Стаття 5 (3) Директиви NIS вимагає від держав-членів ЄС скласти перелік основних послуг, що базуються на цих секторах, підгалузях та типах організацій. Визначені Директивою мінімальні вимоги до гармонізації дають державам-членам змогу вийти за рамки Додатку II та здійснити ідентифікацію в додаткових секторах і підсекторах.

Таблиця 2. Перелік секторів, відповідних галузей і типів суб'єктів, які мають значення для процесу ідентифікації операторів основних послуг

Сектор	Підсектор
1. Енергетика	. (a) Електроенергія; . (b) нафта; . (c) газ
2. Транспорт	. (a) Повітряний транспорт; . (b) залізничний транспорт; . (c) водний транспорт; . (d) автомобільний транспорт
3. Банківська справа	
4. Інфраструктура фінансового ринку	
5. Сектор охорони здоров'я	
6. Постачання та розподіл питної води	
7. Цифрова інфраструктура	

Стаття 5 (2) визначає для держав-членів три критерії ідентифікації операторів основних послуг:

1. Суб'єкт, що займається відповідним питанням, повинен надавати послугу, яка має важливе значення для забезпечення критичної суспільної та / або економічної діяльності. З цією метою національні компетентні органи мають ознайомитися зі своїми раніше складеними списками основних послуг.
2. Надавана послуга має залежати від мережевих та інформаційних систем.
3. Інцидент мусить тягнути за собою значні руйнівні наслідки для надання відповідної послуги.

Згідно зі Статтею 6, значущість інцидента визначається за допомогою міжгалузевих факторів та, де це доцільно, факторів, що стосуються сектора.

Крім того, стаття 5 (4) Директиви NIS зобов'язує держави-члени брати участь у спільних консультаціях, якщо вони виявлять, що потенційний ООП надає послуги у більш ніж одній державі-члені. Цей обов'язковий порядок покликаний допомогти державам-членам оцінити потенційний вплив кіберінцидента, що зачіпає суб'єктів, які працюють за кордоном, а також слугує гарантією для компаній, постраждалих від процедури в різних державах-членах.

Директива NIS пропонує запровадити систему управління ризиками серед компаній або інших суб'єктів, що надають основні послуги, визначені відповідно до статті 5.. Оператори, які підпадають під дію Директиви NIS, зобов'язані вживати відповідних та пропорційних технічних і організаційних заходів для управління ризиками, пов'язаними з безпекою їхніх мережевих та інформаційних систем, і повідомляти про серйозні інциденти компетентним органам.

Відповідно до статті 23 (1) Директиви NIS, у звіті[41] щодо оцінки узгодженості підходів, застосованих державами-членами для визначення операторів основних послуг, оцінюється послідовність підходів, застосованих державами-членами для ідентифікації операторів основних послуг. Оскільки послідовність ідентифікації ООП та ризик фрагментації внутрішнього ринку в цій галузі тісно пов'язані, звіт також містить ширшу оцінку Директиви NIS, як це передбачено у статті 23 (2), яка зобов'язує Єврокомісію періодично переглядати загальне функціонування Директиви та оцінювати перелік секторів і підгалузей, що підлягають ідентифікації ООП та видів цифрових послуг, на які поширюється Директива. Перші такі звіти мають бути подані до 9 травня 2021 року.

Звіт ЄК Європейському Парламенту та Раді щодо оцінки узгодженості підходів, застосованих державами-членами для визначення операторів основних послуг, відповідно до статті 23 (1) Директиви NIS, містить інформацію щодо того, що до вересня 2019 року всі 28 держав-членів повідомили про повну імплементацію Директиви NIS; при цьому у висновках звіту наголошено на певних прогалинах в імплементації.

41 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546

Аналіз показав, що Директива NIS стала каталізатором змін інституційного та регуляторного ландшафту щодо кібербезпеки у багатьох державах-членах. Обов'язок ідентифікувати операторів основних послуг стимулював всебічне оцінювання ризиків, пов'язаних із операторами, що здійснюють критично необхідну для суспільства діяльність, а також із сучасними мережевими та інформаційними системами, майже у всіх державах-членах. Автори звіту визначили це як досягнення для країн-членів ЄС у цілому відповідно до цілей Директиви NIS.

Європейська Комісія задля цього звіту вивчила національні методології ідентифікації послуг, які національні органи вважають істотними, ідентифікаційні критерії та кількість ООП, визначених у різних секторах, на які поширюється Директива, і дійшла таких висновків:

- Держави-члени розробили різні методології ідентифікації ООП, визначення основних послуг та встановлення порогових значень. Це може мати негативний вплив на послідовне застосування положень Директиви NIS у всьому Союзі та спричинити ризики для ефективного функціонування внутрішнього ринку й подолання кіберзагроз.
- Держави-члени по-різному витлумачили «основні послуги» відповідно до Директиви NIS, при цьому вони застосовують різні рівні деталізації. Це ускладнює порівняння списків основних послуг. Крім того, з одного боку, виникає ризик фрагментації сфери застосування Директиви NIS; з іншого боку, деякі оператори підпадають під вплив додаткового регулювання (оскільки були визначені відповідною державою-членом), тоді як надання інших аналогічних послуг залишилися без регулювання (бо вони не були ідентифіковані). З метою усунення невідповідностей необхідно з урахуванням досвіду держав-членів здійснити кроки, що допоможуть надалі укласти більш узгоджений перелік основних послуг.

Крім того, у звіті також наголошено на істотних розбіжностях у застосуванні державами-членами порогових значень. Подальше узгодження порогових значень на рівні ЄС може допомогти усунути цю проблему. Наприклад, таку роботу можна проводити за окремими галузями в рамках Групи співробітництва з урахуванням національної специфіки, зокрема особливих вимог малих держав-членів.

Той факт, що деякі країни скористалися можливістю й визначили основні послуги не лише в секторах, окреслених у Додатку II, але й у додаткових секторах чи підсекторах, свідчить: є інші сектори, потенційно вразливі до кіберінцидентів, крім тих, що рекомендовані до розгляду в Директиві NIS. Ідентифікація ООП у таких галузях, як інформаційна інфраструктура, фінансові послуги, які не охоплені суб'єктами, переліченими у Додатку II, та урядом, можуть покращити кіберстійкість організацій у таких секторах. Однак якщо лише деякі з держав-членів визначають ООП у цих секторах, це може негативно позначитися на внутрішньому ринку та рівних умов, які він повинен забезпечити.

Окремо слід звернути увагу на питання об'єктів критичної інфраструктури (ОКІ). У Директиві 114 визначено термін «критична інфраструктура» та встановлено рамки для ідентифікації об'єктів критичної інфраструктури. По суті, ООП у термінах директив є наступниками об'єктів критичної інфраструктури (див. Таблицю 3), оскільки сектори та підсектори повністю збігаються, але є певні інші відмінності, які необхідно врахувати під час імплементації.

Так, додаток II до Директиви NIS для цілей статті 5 визначає ООП за нижченаведеними видами діяльності із посиланням на законодавство ЄС. Це додатково сприяє розтлумаченню критеріїв віднесення підприємств до ООП.

Таблиця 3. Додаток II до Директиви 114. Види діяльності для цілей (4) статті 4

Сектор	Підсектор	Тип організації
1. Енергетика	(a) Електрика	Підприємства з електричної енергії, визначені в пункті (35) статті 2 Директиви 2009/72/ЄС Європейського Парламенту та Ради (1), які виконують функцію «постачання», як визначено у пункті (19) статті 2 цієї Директиви
		Оператори системи розподілу, визначені у пункті 6 статті 2 Директиви 2009/72/ЄС
		Оператори системи передачі, як визначено в пункті 4 статті 2 Директиви 2009/72/ЄС
	(b) Нафта	Оператори нафтопроводів
		Оператори об'єктів з видобутку, переробки та очищення нафти, зберігання та передачі
	(c) Газ	Підприємства з постачання, визначені в пункті 8 статті 2 Директиви 2009/73/ЄС Європейського Парламенту та Ради (2)
		Оператори системи розподілу, визначені в пункті 6 статті 2 Директиви 2009/73/ЄС
		Оператори системи передачі, визначені в пункті 4 статті 2 Директиви 2009/73/ЄС
		Оператори систем зберігання, як визначено в пункті 10 статті 2 Директиви 2009/73/ЄС
		Оператори системи СПГ, як визначено у пункті 12 статті 2 Директиви 2009/73/ЄС
		Підприємства з природного газу, як визначено у пункті 1 статті 2 Директиви 2009/73/ЄС
		Оператори очисних споруд
2. Транспорт	(a) Повітряний транспорт	Авіаперевізники, визначені в пункті 4 статті 3 Регламенту (ЄС) №300/2008 Європейського Парламенту та Ради (3)
		Органи управління аеропортами, визначені в пункті 2 статті 2 Директиви 2009/12/ЄС Європейського Парламенту та Ради (4), аеропорти, визначені в пункті 1 статті 2 цієї Директиви, включно з основними аеропортами, переліченими у розділі 2 Додатка II до Регламенту (ЄС) №1315/2013 Європейського Парламенту та Ради (5), та організації, що експлуатують допоміжні установки, розміщені в аеропортах

Сектор	Підсектор	Тип організації
		Оператори управління дорожнім рухом, що надають послуги з контролю за повітряним рухом (управління повітряним рухом), визначені в пункті 1 статті 2 Регламенту (ЄС) №549/2004 Європейського Парламенту та Ради (6)
	(b) Залізничний транспорт	суб'єкти управління інфраструктурою, визначені в пункті 2 статті 3 Директиви 2012/34/ЄС Європейського Парламенту та Ради (7)
		Залізничні підприємства, визначені в пункті 1 статті 3 Директиви 2012/34/ЄС, включно з операторами служб, визначених у пункті 12 статті 3 Директиви 2012/34/ЄС
	(c) Водний транспорт	Компанії внутрішнього, морського та прибережного пасажирського й вантажного водного транспорту, визначені для морського транспорту в Додатку I до Регламенту (ЄС) №725/2004 Європейського парламенту та Ради (8), без урахування окремих суден, якими керують ці компанії
		Органи управління портами, визначені в пункті 1 статті 3 Директиви 2005/65/ЄС Європейського Парламенту та Ради (9), включно з їхніми портовими спорудами, визначеними в пункті 11 статті 2 Регламенту (ЄС) №725/2004, та суб'єкти, що експлуатують обладнання в портах
		Оператори служб суднового руху, визначені пунктом (o) статті 3 Директиви 2002/59/ЄС Європейського Парламенту та Ради (10)
	(г) Дорожній транспорт	Дорожні органи, визначені в пункті 12 статті 2 Делегованого регламенту Комісії (ЄС) 2015/962 (11), відповідального за контроль управління дорожнім рухом
		Оператори інтелектуальних транспортних систем, як визначено у пункті 1 статті 4 Директиви 2010/40/ЄС Європейського Парламенту та Ради (12)
3. Банківська справа		Кредитні установи, визначені пунктом 1 статті 4 Регламенту (ЄС) №575/2013 Європейського Парламенту та Ради (13)
4. Інфраструктура фінансового ринку		Оператори торгових майданчиків, визначені у пункті (24) статті 4 Директиви 2014/65/ЄС Європейського Парламенту та Ради (14)
		Центральні контрагенти (КПК), визначені пунктом 1 статті 2 Регламенту (ЄС) №648/2012 Європейського Парламенту та Ради (15)
5. Сектор охорони здоров'я	Заклади охорони здоров'я (включно з лікарнями та приватними клініками)	Медичні працівники, визначені пунктом (g) статті 3 Директиви 2011/24/ЄС Європейського Парламенту та Ради (16)
6. Постачання та розподіл питної води		Постачальники та розподілювачі води, призначеної для споживання людиною, як визначено у пункті (1) (a) статті 2 Директиви Ради 98/83/ЄС (17), але без урахування суб'єктів, для яких розподіл води для споживання людиною є лише частиною їхньої діяльності з дистрибуції інших товарів та товарів, які не вважаються основними послугами
		ІХП
		Постачальники послуг DNS
		Реєстри імен TLD

Тому в Україні необхідно буде на рівні закону встановити категорії ООП (ОКІ), критерії захисту та інші, не врегульовані чинним Законом України «Про основні засади забезпечення кібербезпеки України» норми[42], на які звернула увагу Державна регуляторна служба[43].

Слід пам'ятати про важливі норми Директиви NIS та Директиви 114, які передбачають, що захист критичної інфраструктури держави здійснюється у співпраці державних структур та приватних підприємств. Державні органи мають достатні повноваження та адміністративний вплив, але відзначаються великою інерційною бюрократичною складовою і браком дієвої взаємодії, на відміну від приватного бізнесу, що зазвичай швидко реагує на загрози в кіберпросторі, а також має можливості для залучення кращих фахівців до сектора кібербезпеки. Співвідношення завдань державних органів та приватних структур може бути різним. Тому в майбутньому законодавстві України слід детальніше окреслити механізми державно-приватного партнерства (взаємодії) з подальшим переглядом чинних законів про державно-приватне партнерство та концесію.

Документи ЄС пропонують ризик-орієнтований підхід до розробки механізмів і політик убезпечення від кібератак, тероризму, інших кіберзлочинів. При цьому в більшості документів прописані схеми оцінки відповідності, сертифікації на добровільних засадах і великі санкції за втрату конфіденційної інформації.

Обов'язковими заходами захисту ООП (ОКІ) є визначення ризиків та розробка моделі кіберзагроз.

Оцінювання ризиків передбачає визначення потенційних загроз, наслідків цих загроз та розрахунок їх вірогідності. Аналіз ризиків — важливий крок на шляху до побудови ефективної системи управління кризовими ситуаціями та інцидентами. Оцінку ризиків можна проводити на об'єктовому, галузевому та загальнодержавному (національному) рівнях.

Український підхід кардинально відрізняється — зазвичай законодавство встановлює чітке регулювання, при цьому після реформи системи стандартизації і оцінки відповідності сертифікація для даного виду послуг сфери інформаційного суспільства є добровільною.

Аналіз ризиків також може стати базою для іншого механізму забезпечення кібербезпеки — страхування ризиків, яке наразі в даній сфері не застосовується: відсутні розрахунки ризиків, не визначено орган, який може організувати таку діяльність, крім того, чинним законодавством не передбачено можливості страхування кіберризиків у зв'язку з відсутністю ліцензування цього виду страхування.

Технологічні процеси на ОКІ залежать від стану їх кіберзахисту, а порушення функціонування ІТС таких об'єктів може призвести до негативних наслідків для економіки, суспільства, населення та держави в цілому, тому кібербезпека ОКІ має бути основним і пріоритетним напрямом захисту.

42 http://www.drs.gov.ua/wp-content/uploads/2019/11/554.pdf

43 http://www.drs.gov.ua/wp-content/uploads/2019/06/328.pdf

Негативними наслідками надзвичайних подій у кіберпросторі, згідно з національним законодавством, в Україні[44] вважаються:

- виникнення надзвичайної ситуації техногенного характеру та / або негативний вплив на стан екологічної безпеки держави (регіону) (Н.1);
- негативний вплив на стан енергетичної безпеки держави (регіону) (Н.2);
- негативний вплив на стан економічної безпеки держави (Н.3);
- негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н.4);
- негативний вплив на систему управління державою (Н.5);
- негативний вплив на суспільно-політичну ситуацію в державі (Н.6);
- негативний вплив на імідж держави (Н.7);
- порушення сталого функціонування фінансової системи держави (Н.8);
- порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н.9);
- порушення сталого функціонування інформаційної та / або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними структурами інших держав (Н.10).

ОКІ різних галузей економіки справляють різний за масштабами вплив на життєдіяльність країни. Так, наприклад, потужні об'єкти генерації та постачання електроенергії мають загальнодержавне значення, тоді як об'єкти водопостачання охоплюють певну локальну територію або міста. Кодекс цивільного захисту[45] класифікує надзвичайні події залежно від обсягів заподіяних надзвичайною ситуацією наслідків, обсягів технічних і матеріальних ресурсів, необхідних для їх ліквідації. Визначаються такі рівні надзвичайних ситуацій: державний, регіональний, місцевий, об'єктовий. Залежно від характеру походження подій, що можуть зумовити виникнення надзвичайних ситуацій на території України, визначаються такі види надзвичайних ситуацій: техногенного характеру, природного характеру, соціальні, воєнні. Надзвичайні події на ОКІ, викликані кіберагресією, належать до техногенних, але незалежно від причин техногенної надзвичайної події наслідки можуть бути тяжкими, а їх ліквідація відбувається відповідно до рівня загрози. Таким чином, необхідно врегулювати питання визначення окремих надзвичайних подій, які наразі зараховують до техногенних, і виокремлення з них цифрових, або кіберподій.

Директива 114 дає державам-членам ЄС право визначити на національному рівні сектори для імплементації, а базовими секторами названі енергетичний, транспортний та ІКТ. При цьому Директива 114 не обмежує у впровадженні окремих заходів безпеки в інших секторах.

Держави-члени ідентифікують об'єкти критичної інфраструктури відповідно до статті 3.

---

44 https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF

45 https://zakon.rada.gov.ua/laws/show/5403-17

Серед критеріїв, зокрема:

(a) критерій нещасних випадків (оцінюється потенційна кількість смертельних випадків або отриманих травм);

(b) критерій економічних результатів (оцінюється значущість економічних втрат та / або погіршення продуктів чи послуг, зокрема потенційні екологічні наслідки);

(c) критерій суспільних наслідків (оцінюється вплив на суспільну довіру, фізичні страждання, порушення повсякденного життя, зокрема ненадання основних послуг).

Тому перелік секторів європейської критичної інфраструктури сам по собі не породжує загального зобов'язання щодо призначення ОКІ у кожному секторі.

Держави мають визначити безпековий план для власників / операторів ОКІ.

Безпековий план визначатиме об'єкти критичної інфраструктури та рішення для забезпечення безпеки, що вже існують або впроваджуються. Процедура розробки безпекових планів має, серед іншого, охопити:

1) ідентифікацію важливих об'єктів;

2) аналіз ризиків на основі сценаріїв головних загроз, вразливостей кожного об'єкта і його потенційного впливу;

3) ідентифікацію, відбір і встановлення пріоритетності запобіжних заходів і процедур, що поділяються на:
   - постійні заходи забезпечення безпеки, що визначають необхідні рівні фінансування та механізми захисту, які мають застосовуватися на всіх етапах. Цей підпункт включатиме інформацію про загальні заходи: технічні заходи (зокрема встановлення засобів виявлення, контролю доступу, захисту, запобігання); організаційні заходи (зокрема процедури попередження про небезпеку, управління кризами); заходи контролю й верифікації; комунікації; підвищення рівня обізнаності й підготовки; безпеку інформаційних систем;
   - поетапні заходи забезпечення безпеки, що активуються залежно від рівнів ризику і загроз.

Відповідно до статті 3 Директиви 114 кожна держава-член має визначити критичні інфраструктури, застосовуючи низку послідовних кроків.

Потенційна європейська критична інфраструктура, що не відповідає одній чи кільком нижченаведеним вимогам, вважається такою, що «не є європейською критичною інфраструктурою», і виключається з процедури. Потенційна європейська критична інфраструктура ЄКІ, що відповідає вимогам, проходить через наступні кроки цієї процедури[46].

46 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114

КРОК 1 Кожна держава-член має застосувати секторальні критерії під час першого відбору критичної інфраструктури в межах сектора.

КРОК 2 Кожна держава-член має застосувати до потенційної ЄКІ, ідентифікованої на етапі кроку 1, означення критичної інфраструктури відповідно до статті 2(a). Істотність впливу визначається національними методами ідентифікації критичних інфраструктур або за допомогою застосування наскрізних критеріїв на відповідному національному рівні. Для інфраструктури, що надає основну послугу, також беруться до уваги наявність альтернатив та тривалість збою / відновлення.

КРОК 3 Кожна держава-член має застосувати до потенційної ЄКІ, що пройшла два попередні кроки процедури, транскордонний аспект означення ЄКІ відповідно до статті 2(b). До потенційної ЄКІ, що відповідає такому означенню, застосовуватиметься наступний крок цієї процедури. Для інфраструктури, що надає основну послугу, також беруться до уваги наявність альтернатив та тривалість збою/відновлення.

КРОК 4 Кожна держава-член має застосувати наскрізні критерії до решти потенційних ЄКІ. Наскрізні критерії повинні враховувати: ступінь впливу; для інфраструктури, що надає основну послугу, — доступність альтернатив; тривалість збою / відновлення. Потенційна ЄКІ, що не відповідає наскрізним критеріям, не вважатиметься ЄКІ.

Інформацію про потенційну ЄКІ, що пройшла цю процедуру, повідомляють лише тим державам-членам, що можуть зазнати істотного впливу цієї потенційної ЄКІ.

Для України питання потенційних ЄКІ набуде актуальності у зв'язку з можливим приєднанням до Єдиного цифрового ринку ЄС. Тому на рівні законодавства необхідно передбачити підготовку періодичних аудитів щодо визначення потенційних ЄКІ, доповнення їх переліку або вилучення об'єктів із нього.

Що ж до імплементації GDPR та Директиви 680, то на підставі попередніх досліджень необхідно буде узгодити термінологічну базу, законодавчо врегулювати схеми сертифікації для захисту конфіденційної інформації, розробити механізми координації двох регуляторів — з кібербезпеки та захисту персональних даних, визначити рівні захисту, порядок повідомлення про інциденти, встановити відповідальність, розробити окремі механізми для правоохоронних органів, зокрема з метою виконання двох міжнародних угод — із Євроюстом та Європолом.

Інші документи охоплюють окремі аспекти кібербезпеки в певних секторах взаємодії державних структур та фізичних і юридичних осіб під час надання / отримання послуг інформаційного суспільства.

Окремо слід звернути увагу на Регламент електронної конфіденційності, який не був врахований під час підготовки законопроєкту «Про електронні комунікації» (№3014, дата реєстрації 05.02.2020 р.) та потребуватиме узгодження законодавства в частині регулювання сфери електронних комунікацій та визначення особливих вимог щодо кібербезпеки цих комунікацій.

Регламент 1807 забороняє встановлювати на національному рівні у країнах-членах ЄС локалізацію даних (крім персональних даних та якщо така локалізація не обґрунтована міркуваннями громадської безпеки відповідно до принципу пропорційності), сприяє розробці саморегулювальних кодексів поведінки.

Кодекси поведінки мають охопити такі аспекти:

(a) найкращі практики полегшення комутації постачальників послуг та перенесення даних у структурованому, загальновживаному та машиночитаному форматі, включно з відкритими стандартними форматами, якщо цього вимагає постачальник послуг, який отримує дані;

(b) мінімальні вимоги до інформації, завдяки яким професійні користувачі до укладення договору на обробку даних отримують достатньо детальну, чітку та прозору інформацію щодо процесів, технічних вимог, строків та зборів, що застосовуються у випадку, якщо професійний користувач хоче перейти до іншого постачальник послуг або перепортувати дані на власні IT-системи;

(c) підходи до схем сертифікації, які полегшують порівняння продуктів та послуг з обробки даних для професійних користувачів з урахуванням встановлених національних чи міжнародних норм. Такі підходи можуть включати, серед іншого, управління якістю, управління інформаційною безпекою, управління безперервністю бізнесу та управління довкіллям;

(г) дорожні карти комунікацій, що використовують мультидисциплінарний підхід для підвищення обізнаності відповідних заінтересованих сторін із кодексами поведінки.

Тобто Регламенти 1807 та GDPR, Директива NIS та інші документи пропонують такі механізми для державно-приватного партнерства: розробка схем сертифікації, кодексів поведінки та протоколів взаємодії між суб'єктами для кращої комунікації у випадку загроз і інцидентів.

Держави мають призначити єдину «контактну точку» для обміну даними.

Документ, нещодавно підготовлений Європейським судом аудиторів, доводить, що навіть ухвалення Регламентів, що не потребують імплементації на рівні законодавства країн-членів ЄС, не є ефективним заходом: цифрова сфера є надто динамічною, тож потребує постійного аналізу і врегулювання нових і нових викликів.

Як зазначено у звіті, «прагнення ЄС з 2017 року активізувати зусилля щодо зміцнення кібербезпеки та його цифрової автономії справді є доречним і вчасним»[47].

Звіт не є класичним аудиторським звітом, заснований на загальнодоступній інформації та мав на меті забезпечити огляд складного й нерівномірного ландшафту політики та визначити основні проблеми задля забезпечення ефективної реалізації політики. Звітом охоплено такі питання: регулювання політики кібербезпеки ЄС, кіберзлочинність і кіберзахист, а також зусилля у боротьбі з дезінформацією.

47 https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=49416

Визначені у звіті проблеми згруповані за такими масштабними темами:

(I) політика та законодавча база;

(II) фінансування й витрати;

(III) забезпечення кіберстійкості;

(IV) ефективне реагування на кіберінциденти.

У кожному розділі наведено міркування щодо зазначених викликів.

На думку авторів звіту, заходи на виконання загальних цілей стратегії кібербезпеки ЄС мали сформувати найбезпечніше цифрове середовище у світі, але проблемою є відсутність вимірюваних цілей та обмеження достовірних даних. Крім того, бракує оцінювання результатів та різних сфер політики.

Отже, на думку авторів звіту, ключовими викликами для екосистеми кібербезпеки ЄС є:

- забезпечення змістовної підзвітності та оцінки — за допомогою переходу до культури ефективності із вбудованими методами оцінювання;
- прогалини та непослідовні зміни законодавства;
- різний рівень інвестицій у країнах ЄС, зокрема спрямованих на ефективніше використання результатів наукових досліджень та забезпечення дієвого таргетування й фінансування стартапів;
- чітке визначення витрат на реалізацію Стратегії кібербезпеки ЄС;
- посилення ролі агентств ЄС, підвищення кваліфікації та професійності осіб, які здійснюють управління кібербезпекою;
- розкриття інформації щодо стандартів, навчання, сертифікації або оцінок кіберризиків з метою посилення навичок кібербезпеки;
- посилення координації зусиль держав-членів, органів і суспільства для забезпечення кібербезпеки;
- покращення обміну інформацією та координації між державним і приватним секторами;
- інтеграція кібербезпеки в наявні механізми координації реагування на кризи на рівні ЄС;
- посилення захисту критичної інфраструктури та функцій суспільства;
- убезпечення від потенційного втручання у виборчі процеси та дезінформаційних кампаній.

ДОКУМЕНТИ НАТО

Співпрацю України з НАТО в частині обміну інформацією розкрито в двох документах — Угоді з НАТО[48] та Адміністративних домовленостях[49]. Відповідно до статті 4 Угоди про безпеку, Адміністративні домовленості, що стосуються охорони та поводження з інформацією з обмеженим доступом, обмін якою здійснюється між Україною та НАТО, погоджено з урахуванням національного законодавства України у сфері охорони та поводження з інформацією з обмеженим доступом та мінімальних стандартів безпеки, затверджених у документі «Політика безпеки НАТО» (C-M(2002)49), а також її підтримуючих директивах (зі змінами).

Політика безпеки НАТО розроблена на підставі стандартів і директив. Україна є країною, що прагне членства в НАТО, а в частині безпеки інформації має виконати такі дії: «після приєднання запровадить достатні засоби безпеки та процедури для гарантування захисту найбільш засекреченої інформації відповідно до положень політики НАТО з питань безпеки інформації»[50].

Угоди України з країнами-членами НАТО (Польщею, Румунією, Португалією, Іспанією, Естонією, Словенією, Латвією, Литвою, Грецією, Болгарією, Францією) в частині співпраці щодо обміну інформацією та її охорони були підписані після підписання Угоди з НАТО.

Угоди є типовими і визначають дипломатичний канал передачі інформації та паперовий обіг між країнами.

48 https://zakon.rada.gov.ua/laws/show/950_002

49 https://zakon.rada.gov.ua/laws/show/950_035-16

50 https://ukraine-nato.mfa.gov.ua/pro-nato/politika-vidkritih-dverej-ta-plan-dij-shchodo-chlenstva-v-nato

Директиви НАТО, що потребують імплементації в національне законодавство в частині обміну і безпеки інформації :

- AC/35-D/2000-REV7 Directive on Personnel Security (Директива з безпеки персоналу) [51];
- AC/35-D/2002-REV4 Directive on the Security of Information (Директива з безпеки інформації)[52];
- AC/35-D/2003-REV4 Directive on Industrial Security (Директива з безпеки виробництва)[53];
- AC/35-D/2004-REV3 Primary Directive on CIS Security (Первинна директива з безпеки КІС)[54];
- AC/35-D/2005-REV3 Management Directive on CIS Security (Директива з управління безпекою КІС)[55];
- AC/35-D2001-REV2 Directive on Physical Security (Директива з фізичної безпеки)[56].

Оскільки основною метою цього документу є огляд законодавства ЄС з питань кібербпезпеки, детально зупинятися на директивах НАТО тут недоцільно. Зазначимо, що паперовий обіг на сьогодні в Україні регулюється низкою законів і постанов Кабінету Міністрів України — Законами України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», Постановою Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» №373 від 29 березня 2006 р. Додатково можна ознайомитися з детальним оглядом[57] із дотичного питання та запропонованим для врегулювання цих питань законопроєктом [58], у якому частково враховано норми, що потребують імплементації, зокрема ризик-орієнтований підхід, про який вже йшлося вище, та запровадження сертифікаційних процедур для систем обробки інформації, що потребує захисту.

51 http://www.dksi.bg/NR/rdonlyres/852F2C9E-7CC8-441B-A63A-4A456D42E59D/0/Personnel_SecurityAC35D2000REV7.pdf

52 http://www.dksi.bg/NR/rdonlyres/DA629957-ECB2-40D6-9094-0F20396E5780/0/Information_SecurityAC35D2002REV4.pdf.

53 http://www.jftc.nato.int/images/budfin/ac-35-d-2003-rev4.pdf

54 http://www.dksi.bg/NR/rdonlyres/6DC49C44-5C52-47A2-8773-6BF11C59E53C/0/Primary_CIS_SecurityAC35D2004REV3.pdf

55 https://www.nbu.cz/download/pravni-predpisy---nato/AC_35-D_2005-REV3.pdf

56 http://www.dksi.bg/NR/rdonlyres/9D0EE24C-86D9-4C90-8084-70F5BC14B03B/0/Physical_SecurityAC35D2001REV2.pdf

57 http://zbirnyk-nadu.academy.gov.ua/article/download/187133/186457

58 http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=319262&cat_id=317163

РЕЗУЛЬТАТИ КОМУНІКАЦІЇ ТА СПІВПРАЦІ УКРАЇНИ І ЄС

У липні 2018 року Верховна Рада України ухвалила постанову, в якій закликала інституції Європейського Союзу сприяти максимальному використанню можливостей інтеграції України до внутрішнього ринку Європейського Союзу, «включаючи питання формування оновленого порядку денного співробітництва між Україною та Європейським Союзом у сферах юстиції, свободи та безпеки»[59], зокрема сформувати спільне бачення шляхів інтеграції України до Єдиного цифрового ринку ЄС (ЄЦР ЄС).

За підсумками Саміту Україна — ЄС 9 липня 2018 р. Рада асоціації між Україною та Європейським Союзом погодилася продовжити діалог, що випливає з ініціативи України **поглибити співробітництво** в рамках Угоди про асоціацію в таких галузях, як енергетика, юстиція і внутрішні справи, митниця та цифрова економіка, а також розпочати роботу з оновлення, за потреби, додатків до Угоди про асоціацію з метою сприяння процесу імплементації, узгодженому з розвитком права ЄС та відповідних міжнародних стандартів[60].

Восени 2018 року уряд України підготував проєкт Стратегії інтеграції України до ЄЦР ЄС («дорожню карту») та план заходів з її реалізації протягом 2018–2023 років з урахуванням оновлених актів ЄС, що не увійшли як обов'язкові для імплементації до Угоди про асоціацію.

Наприкінці 2018 року ЄС привітав прагнення України надалі наближати своє законодавство до acquis ЄС у сфері цифрової економіки.

59 https://zakon.rada.gov.ua/laws/show/2490-19

60 https://www.kmu.gov.ua/news/rada-asociaciyi-ukrayina-yes-pidtverdila-nezminnu-prihilnist-storin-politichnij-ta-ekonomichnij-integraciyi-zayava-za-pidsumkami-zasidannya

8 липня 2019 року у Києві відбувся 21-й Саміт Україна — Європейський Союз. ЄС привітав прагнення України до подальшого зближення її законодавства із законодавством ЄС у сфері цифрової економіки. Україна та ЄС висловили сподівання щодо подальшої регулярної взаємодії, зокрема здійснення Європейським Союзом двоетапної оцінки нормативно-правового наближення України.

ЄК запустила тривалий процес оцінювання проєкту Стратегії інтеграції України до ЄЦР ЄС та узгодження окремих пропозицій. У серпні 2019 року в Україні розпочала свою діяльність місія ЄС з оцінки наближення нормативно-правового регулювання українського цифрового ринку. На перших зустрічах було відзначено високий рівень зацікавленості усіх стейкхолдерів у досягненні конкретних результатів та переході до наступного етапу двостороннього діалогу: формування Спільного плану дій Україна — ЄС у цифровій сфері.

Експерти місії мали працювати в Києві до кінця 2019 року, але наразі строк місії продовжено до кінця квітня 2020 року. Основна увага місії зосереджена на секторі телекомунікаційних послуг, оскільки Угода про асоціацію містить чіткі зобов'язання щодо імплементації декількох директив ЄС у цій царині, на відміну від інших секторів цифрового ринку. Місія планувала провести аналіз чинного національного законодавства у сфері електронних комунікацій, радіочастотного ресурсу, електронної ідентифікації та електронної торгівлі, відповідних проєктів законів, які прийняті, зареєстровані або будуть зареєстровані у Верховній Раді України. Особливу увагу буде приділено плану імплементації у контексті інституційної спроможності регулятора у сфері електронних комунікацій. Зазначені компоненти становлять технологічну основу Єдиного цифрового ринку ЄС.

Триває комунікація з ЄС щодо імплементації Директиви NIS, оскільки вона не включена в додатки до Угоди про асоціацію, так само як і Регламент GDPR. Уряд України наразі шукає рішення, які влаштують обидві сторони Угоди.

РЕКОМЕНДАЦІЇ ЩОДО КОРИГУВАНЬ, ЯКІ СЛІД ЗДІЙСНИТИ В УКРАЇНІ

З метою покращення взаємодії з європейськими інституціями та наближення внутрішніх політик до європейських Україні необхідно здійснити нижченаведені заходи, законодавчі, організаційні та фінансові.

І. ЗАКОНОДАВЧІ ЗАХОДИ

З огляду на необхідність урегулювання великої кількості питань із різними сферами пропонується розробити кілька проєктів законів — про кібербезпеку (запропоновану автором концепцію майбутнього проєкту закону, яку вже обговорює робоча група при Комітеті Верховної Ради з питань цифрової трансформації, наведено в Додатку 1); проєкт закону про об'єкти критичної інфраструктури; проєкт закону про внесення змін до Кримінального Кодексу України в частині повної імплементації Конвенції про кіберзлочинність (щодо електронних доказів); проєкт закону про регулятора в сфері кібербезпеки; проєкт закону про безпеку інформації. Перелік не є вичерпним, а узгодження терміносистем України та ЄС потребуватиме внесення змін до інших чинних законів України — «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних»; уточнення термінів «конфіденційна інформація» та «комерційна таємниця».

Таким чином, заходи, що потребують законодавчого врегулювання:

- Приведення терміносистеми у сфері кібербезпеки у відповідність до визначень міжнародних практик: коригування наявних та впровадження нових термінів з урахуванням законодавства та європейських і міжнародних стандартів у цій сфері;

- визначення регулятора сфери кібербезпеки;
- визначення принципів взаємодії учасників забезпечення кібербезпеки та їхніх прав і обов'язків;
- визначення меж саморегулювання для інших — недержавних — суб'єктів кібербезпеки. З метою забезпечення державно-приватного партнерства необхідно визначити можливості для саморегулювання у певних сферах та участі у розробці державної політики у сфері захисту ОКІ;
- визначення механізмів взаємодії, повідомлення та обміну інформацією в разі кіберінцидента від ОКІ до єдиної точки взаємодії, зокрема процедур звітування про результати їх оброблення та убезпечення.
- встановлення вимог до CSIRT (додаток 1 до Директиви NIS);
- визначення порядку акредитації в Україні та прийняття акредитації CSIRT, здійсненої в ЄС, CERT тощо;
- розширення сфери дії майбутнього закону на діяльність, пов'язану з обробкою інформації, що становить державну таємницю, засобами інформаційно-комунікаційних технологій, шляхом запровадження окремої процедури оцінки виконання заходів з кібероборони під час акредитації з безпеки інформаційно-комунікаційних систем;
- розширення переліку до принципів забезпечення кібербезпеки таким: «проведення на постійній основі періодичного аналізу результативності заходів із забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів силами персоналу цих об'єктів та із залученням уповноважених організацій у цій сфері, зокрема волонтерських організацій та їх об'єднань, які акредитовані у встановленому порядку (або внесені до реєстру виконавців робіт із захисту інформації відповідно до Закону України «Про безпеку інформації та інформаційно-комунікаційних систем»[61])»;
- визначення загальних принципів огляду національної системи кібербезпеки та критичної інформаційної інфраструктури;
- створення передумов для страхування ризиків, при цьому визначення на базі ризик-орієнтованого підходу критичних ризиків, що можуть підлягати обов'язковому страхуванню;
- визначення особливостей захисту певних видів інформації (конфіденційних, службових даних тощо);
- розробка нового проєкту закону про об'єкти критичної інфраструктури на базі вже підготовлених проєктів законів (проєкт уже опрацьовує робоча група при Комітеті з питань цифрової трансформації)[62];

61 http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=319256&cat_id=38837&ctime=1583911712891

62 https://drive.google.com/drive/folders/1bkMRCdNDMD4wDpDsT0n0CK--RegzKPl7

- запровадження галузевого принципу формування переліку ОКІ та встановлення галузевими регуляторами правил і норм дотримання принципів кібербезпеки у галузях, якими вони опікуються;
- визначення на законодавчому рівні основних видів цифрових послуг, що мають критичне значення для національної безпеки, при цьому надання Кабінету Міністрів України змоги визначати на рівні технічних регламентів вимоги до їх надання.

II. РОЗРОБКА СТРАТЕГІЇ З КІБЕРБЕЗПЕКИ

Цей рік є перехідним для чинної Стратегії з кібербезпеки, що розроблялася на період до 2020 року; додатковий чинник — статті 26 і 31 Закону України «Про національну безпеку», які визначають порядок розробки Стратегії національної безпеки та Стратегії кібербезпеки України: «Організація підготовки Стратегії кібербезпеки України здійснюється за дорученням Президента України Національним координаційним центром кібербезпеки **після затвердження** Стратегії національної безпеки України»[63].

З огляду на необхідність імплементації європейського законодавства та узгодження двох різних підходів до кібербезпеки слід розробити нову Стратегію кібербезпеки з окремим розділом щодо мережевої та інформаційної безпеки й, відповідно, етапів, цілей і показників досягнення, запропонованих ENISA.

У самій Стратегії кібербезпеки України необхідно окреслити основні принципи планування, бюджетування, виконання та аналізу ефективності заходів з виконання Стратегії кібербезпеки України, що не мають суперечити заходам і принципам, визначеним законами.

На рівні закону чи підзаконних актів необхідно визначити механізми підготовки та оцінки виконання Стратегії з кібербезпеки на підставі рекомендацій ENISA.

ENISA рекомендує шість етапів розробки національної стратегії з кібербезпеки:

- окресліть бачення, обсяг, цілі та пріоритети;
- визначте підходи до оцінки ризику;
- оцініть чинну політику, правила та можливості;
- визначте чітку структуру управління;
- визначте та залучіть заінтересовані сторони;
- створіть надійні механізми обміну інформацією.

63 https://zakon.rada.gov.ua/laws/show/2469-19

Крім того, ENISA рекомендує п'ятнадцять цілей впровадження Національної стратегії з кібербезпеки:

- розробити національні плани на випадок надзвичайних ситуацій;
- забезпечити захист критичної інформаційної інфраструктури;
- організувати тренінги з кібербезпеки;
- запровадити базові заходи безпеки;
- створити механізми звітування про інциденти;
- підвищити рівень обізнаності користувачів;
- посилити навчальні та освітні програми;
- забезпечити здатність реагувати на інцидент;
- визначити адресу для повідомлення про злочини;
- провадити міжнародну співпрацю;
- запровадити державно-приватне партнерство;
- забезпечити баланс і конфіденційність;
- інституціоналізувати співпрацю між державними установами;
- забезпечити підтримку наукових досліджень;
- заохочувати приватний сектор інвестувати в заходи безпеки.

Показниками ефективності стратегії кібербезпеки є

- наявність стратегічного національного плану кіберзахисту (теорії, концепції, зацікавлені сторони, конкретні обов'язки);
- ступінь участі в ініціативах ЄС у сфері кіберзахисту (створення потенціалу);
- ідентифікація та структура військової CERT (цілі CERT, рівень військової політики);
- проведення тренувань (для персоналу, якому це необхідно) та рівень впливу;
- оперативна сумісність (можливість взаємодіяти з іншими сторонами);
- підвищена стійкість завдяки співпраці та новим заходам проти військових кібератак (швидше виявлення, реакція і відновлення після складних атак, економічно ефективний розвиток через співпрацю, надійність, доступність та чіткість каналів зв'язку);
- національна інституційна основа для боротьби з кіберзлочинністю (LEAs, CERTs тощо);
- забезпечення виконання LEA (аналіз прогалин, ідентифікація потреби, сучасні технічні засоби, найкращі практики використання);
- наявність механізмів співпраці з Європолом, Євроюстом, іншими міжнародними організаціями;

- розгляд національних справ про кіберзлочинність;
- міжнародне співробітництво:
  - посилені можливості транскордонної боротьби з кіберзлочинністю;
  - зниження бар'єрів для проведення досліджень;
  - доступ до найсучасніших інструментів;
  - зменшення вартості боротьби з кіберзлочинністю;
- безпечний кіберпростір для всіх користувачів (захищеність користувачів від кіберзлочинів).

III. ОРГАНІЗАЦІЙНІ ЗАХОДИ

Критично важливі заходи, що потребують розгляду й урегулювання, — це забезпечення необхідними людськими, фінансовими й технічними ресурсами для реалізації вимог майбутнього законодавства.

Запровадження будь-якого законодавства на рівні ЄС зазвичай супроводжується аналізом регуляторного впливу і попередньою оцінкою вжитих заходів, що не були ефективними, на підставі наперед розробленої методики чи системи оцінки.

Державна регуляторна служба України неодноразово звертала увагу на відсутність аналізу регуляторного впливу під час підготовки проєктів законів і постанов Кабінету Міністрів України у сфері забезпечення кібербезпеки. Але ця норма не виконується, зокрема, й через брак необхідних ресурсів у органа, який сьогодні формує державну політику в сфері кібербезпеки.

Тому в процесі підготовки нового законодавства необхідно передбачити механізми фінансування, серед іншого,аналізу регуляторного впливу чи оцінки ефективності виконання стратегії кібербезпеки та інших законів.

Щодо створення системи захисту ОКІ: розпорядженням Кабінету Міністрів України від 6 грудня 2017 року №1009-р схвалено Концепцію створення державної системи захисту критичної інфраструктури.

У цьому документі визначено такі основні проблеми, що потребують розв'язання:

- відсутність єдиної загальнодержавної системи захисту критичної інфраструктури;
- недостатність та неузгодженість нормативно-правового регулювання з питань захисту систем і об'єктів критичної інфраструктури, зокрема відсутність спеціального закону про критичну інфраструктуру та її захист;

- відсутність державного органа, відповідального за координацію дій у сфері захисту критичної інфраструктури;
- невизначеність повноважень, завдань і відповідальності центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників (розпорядників) об'єктів критичної інфраструктури;
- відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації;
- відсутність єдиної методології проведення оцінки загроз критичній інфраструктурі, а також відсутність спеціального правоохоронного органа, відповідального за проведення аналізу та оцінки загроз критичній інфраструктурі внаслідок проведення іноземними державами економічної експансії та дискримінаційної політики, недопущення заподіяння шкоди економічному і науково-технічному потенціалу держави, а також організацію та вжиття відповідних заходів протидії;
- нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури та невизначеність джерел фінансування заходів із захисту критичної інфраструктури;
- недостатній рівень міжнародного співробітництва у сфері захисту критичної інфраструктури[64].

В Україні немає на сьогодні єдиного органа, який може координувати діяльність із забезпечення кібербезпеки. Така функція покладена на РНБО — координаційний орган з питань національної безпеки і оборони при Президентові України, який координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони відповідно до статті 107 Конституції України.

Центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, кіберзахисту телекомунікацій і користування радіочастотним ресурсом України, є Адміністрація Державної служби спеціального зв'язку та захисту інформації України. При тому діяльність цього органа зі спеціальним статусом спрямовується і координується Кабінетом Міністрів України через віце-прем'єр-міністра — міністра цифрової трансформації. Але особливість у тому, що цей орган має «подвійне призначення» — є органом виконавчої влади і «складовою сектора безпеки і оборони України»[65] і не може повною мірою виконувати роль регулятора сектора.

Вважаємо за необхідне розробити нову модель системи органів забезпечення кібербезпеки й кіберзахисту з чітким розподілом повноважень і протоколом взаємодії між складовими системи у виконавчій владі й секторі безпеки та оборони.

64 https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80

65 https://zakon.rada.gov.ua/laws/show/3475-15

Також необхідно розробити загальнодержавну цільову програму з кібербезпеки, яка має передбачити як організаційні, так і фінансові ресурси.

Українське бачення в цілому збігається з європейським в частині того, що саме необхідно врегулювати, але в традиціях нормотворення поки не передбачено норм щодо постійного регулярного аналізу, перегляду й удосконалення законодавства.

Більшість законодавчих документів ЄС, на відміну від українських, містять пряму норму про постійний перегляд і оцінювання як регулювання, так і заходів на його виконання, вжитих державами-членами ЄС.

Тому на рівні і законодавства, і Стратегії кібербезпеки необхідно визначити механізми перегляду й оцінки заходів, спрямованих на виконання цілей і завдань.

Україна має можливість імплементувати необхідні норми з урахуванням європейського досвіду й уникнути певних помилок задля забезпечення належного рівня кібербезпеки.

ДОДАТОК 1

КОНЦЕПЦІЯ ПРОЄКТУ ЗАКОНУ ПРО КІБЕРБЕЗПЕКУ

Концепція проєкту закону про кібербезпеку

ЗАКОН УКРАЇНИ

Про кібербезпеку України

Преамбула

РОЗДІЛ І
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

Привести терміносистему у сфері кібербезпеки у відповідність до визначень міжнародних практик: відкоригувати наявні та впровадити нові терміни з урахуванням законодавства та європейських і міжнародних стандартів у цій сфері.

Стаття 2. Сфера застосування закону

Розширити сферу дії майбутнього закону на діяльність, пов'язану з обробкою інформації, що становить державну таємницю, засобами інформаційно-комунікаційних технологій, за допомогою запровадження окремої процедури оцінки виконання заходів з кібероборони під час здійснення акредитації з безпеки інформаційно-комунікаційних систем.

Стаття 3. Принципи забезпечення кібербезпеки

Розширити перелік принципів забезпечення кібербезпеки таким: «проведення на постійній основі періодичного аналізу результативності заходів із забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів силами персоналу цих об'єктів та із залученням уповноважених організацій у цій сфері, зокрема волонтерських організацій та їх об'єднань, які акредитовані у встановленому порядку (або внесені до реєстру виконавців робіт із захисту інформації відповідно до Закону України «Про безпеку інформації та інформаційно-комунікаційних систем»)»[66].

Стаття 4. Цілі і мета Закону

Стаття 5. Міжнародні зобов'язання України у сфері кібербезпеки

Міжнародне співробітництво у сфері кібербезпеки.

РОЗДІЛ II

ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стаття 6. Об'єкти кібербезпеки

Стаття 7. Об'єкти критичної інфраструктури

Порядок віднесення до ОКІ.

Запровадити галузевий принцип формування переліку ОКІ та ОКІІ та встановлення галузевими регуляторами правил і норм дотримання принципів кібербезпеки в галузях, якими вони опікуються.

Визначити на рівні закону основні види цифрових послуг, що мають критичне значення для національної безпеки, при цьому надати можливість Кабінету Міністрів України визначати на рівні технічних регламентів вимоги до їх надання.

Стаття 8. Суб'єкти забезпечення кібербезпеки

Основні суб'єкти забезпечення кібербезпеки, визначені чинним законодавством, не виправдали свого особливого статусу.

Стаття 9. Права і обов'язки суб'єктів забезпечення кібербезпеки

Стаття 10. Національна система кібербезпеки

Багато завдань поставлено перед державним сектором, при цьому більшість об'єктів критичної інфраструктури перебувають у приватному секторі. Відповідальність щодо їх захисту покладена на власників об'єктів критичної інфраструктури, а не на операторів, які фактично можуть забезпечити захист інфраструктури.

Стаття 11. Взаємодія суб'єктів забезпечення кібербезпеки

66 http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=319256&cat_id=38837&ctime=1583911712891

Стаття 12. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA

Стаття 13. Відомчі CERT (SCIRT)

Визначити механізми взаємодії, повідомлення та обміну інформацією в разі кіберінцидента від ОКІ до єдиної точки взаємодії, зокрема процедур звітування про результати їх оброблення та убезпечення.

Встановити вимоги до CSIRT (додаток 1 до Директиви NIS).

Стаття 14. Приватні CSIRT

Визначити порядок акредитації в Україні та прийняття акредитації CSIRT, здійсненої в ЄС, FIRST, CERT тощо.

Стаття 15. Загальні принципи проведення огляду національної системи кібербезпеки та критичної інформаційної інфраструктури

РОЗДІЛ ІІІ

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО

Стаття 16. Взаємодія суб'єктів забезпечення кібербезпеки та CSIRT

Стаття 17.Співпраця сектора безпеки і оборони з іншими суб'єктами забезпечення кібербезпеки

Стаття 18. Основні засади саморегулювання сфери забезпечення кібербезпеки

З метою забезпечення державно-приватного партнерства визначити можливості для саморегулювання у певних сферах та можливість участі у розробці державної політики у сфері захисту ОКІ.

Стаття 19. Інформаційно-аналітичні системи підтримки ухвалення управлінських рішень

Створення та використання інформаційно-аналітичних систем підтримки ухвалення управлінських рішень, зокрема в умовах криз та кризового реагування, порядок повідомлення.

Стаття 20. Взаємодія з міжнародними організаціями

Взаємодія з ENISA та ICANN.

Стаття 21. Обмін інформацією між суб'єктами забезпечення кібербезпеки

Стаття 22. Організація пошуку вразливостей на об'єктах кібербезпеки

Пошук вразливостей як об'єктів критичної інфраструктури, так і інших інформаційно-телекомунікаційних систем державного і приватного сектора. Межа між пошуком вразливостей і складом злочину відповідно до статті 361 Кримінального кодексу України «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» майже відсутня — немає можливості «законного втручання».

Стаття 23. Компенсація збитків, завданих кібератаками

РОЗДІЛ IV

ФІНАНСУВАННЯ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Стаття 24. Принципи планування, бюджетування, виконання та аналізу ефективності заходів із кібербезпеки та Стратегії кібербезпеки України

Окреслити основні принципи планування, бюджетування, виконання та аналізу ефективності заходів з виконання Стратегії кібербезпеки України регулятором у цій сфері, при цьому наголосити, що всі суб'єкти забезпечення кібербезпеки можуть брати участь у цих заходах, пройшовши акредитацію, якщо вони не є основними елементами національної системи кібербезпеки, до яких треба долучити CSIRT.

Стаття 25. Фінансування заходів із забезпечення захисту ОКІ

Стаття 26. Державна цільова програма забезпечення кібербезпеки

Стаття 27. Страхування ризиків

Створити передумови для страхування ризиків, при цьому визначивши на базі ризик-орієнтованого підходу критичні ризики, що можуть підлягати обов'язковому страхуванню.

РОЗДІЛ V.

КОНТРОЛЬ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Стаття 28. Оцінка ефективності забезпечення кібербезпеки в Україні

Щорічне опитування зацікавлених сторін у сфері кібербезпеки.

Стаття 29. Проведення незалежного аудиту діяльності суб'єктів національної кібербезпеки

Рахункова палата як незалежний аудитор для сектора безпеки та оборони.

Незалежний аудит для інших.

Стаття 30. Парламентський контроль у сфері забезпечення кібербезпеки

Чіткі повноваження реагування на розгляд питань на рівні Верховної Ради України (наприклад, право на звернення до Президента з рекомендацією щодо відставки осіб, призначених ним у секторі безпеки та оборони).

Стаття 31. Громадський контроль у сфері забезпечення кібербезпеки

Стаття 32. Державний контроль (регулятор)

РОЗДІЛ VI

ВІДПОВІДАЛЬНІСТЬ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Стаття 33. Адміністративно-господарська відповідальність

Стаття 34. Відповідальність за порушення законодавства у сфері кібербезпеки

Відповідальність за невиконання вимог щодо захисту об'єктів критичної інфраструктури.

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Внесення змін до Закону Україні «Про інформацію». Визначити особливості захисту певних видів інформації.
2. Внесення змін щодо електронних доказів (повна імплементації Конвенції з кіберзлочинності).
3. Розповсюдження обов'язкової акредитації з безпеки тільки на ІТС, що обробляють державну таємницю, службову інформацію, та на об'єкти критичної інформаційної інфраструктури.
4. Встановлення вимог з безпеки інформації за ризик-орієнтованою моделлю.