

ПРИЗНАЧЕНО ДЛЯ ВКАЗАНИХ АДРЕСАТІВ, НЕ ДЛЯ ПУБЛІЧНОГО РОЗПОВСЮДЖЕННЯ

№ 25 – 16
16 січня 2025 року

Народному депутату України,
Голові Комітету Верховної Ради України
з питань цифрової трансформації
Крячку М. В.

Народному депутату України,
Голові Комітету Верховної Ради України
з питань інтеграції України до
Європейського Союзу
Климуш-Цинцадзе І. О.

Народному депутату України,
Голові Комітету Верховної Ради України
з питань антикорупційної політики
Радіній А. О.

Народному депутату України,
Голові Комітету Верховної Ради України
з питань економічного розвитку
Наталусі Д. А.

Щодо проекту Закону №12207

Шановні пані та панове!

Від імені Ради директорів та компаній-членів Американської торговельної палати в Україні (далі – Палата) засвідчуємо вам глибоку повагу та звертаємося щодо наступного.

11 жовтня 2024 року у Верховній Раді України було зареєстровано проект Закону України №12207 «Про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки» (далі – законопроект).

Експерти компаній-членів Палати звертаються до вас з проханням не підтримувати законопроект з огляду на пояснення та обґрунтування, що додаються до цього листа. У разі необхідності експерти компаній-членів Палати готові експертно долучитися до подальшого доопрацювання законопроекту з метою формування збалансованого державного регулювання в майбутньому, яке буде враховувати інтереси держави, бізнесу та потреби суспільства.

У разі виникнення будь-яких запитань щодо цього звернення, просимо вас визначити відповідальну особу, яка зможе звернутися за номером +380952839928 та електронною адресою ivasyukivska@chamber.ua, контактна особа – Інна Васильківська, молодший менеджер Палати з питань стратегічного розвитку.

Додаток: згадане, на 2 арк.

З глибокою повагою,

Президент

Андрій Гундер

Цей документ та інформація, що міститься у ньому, є конфіденційними та призначені виключно для адресатів, зазначених на першій сторінці цього документа. Без попередньої письмової згоди Департаменту комунікацій Палати за електронною адресою pr@chamber.ua забороняється публічне поширення цього документа чи будь-якої його частини.

Рада директорів: Олена Кошарна, Horizon Capital – Голова; Олександр МакУортер, Citi – Заступник голови; Арвід Тюркнер, EBRD – Заступник голови; Сергій Мартинчук, Cisco – Скарбник; Сергій Чорний, Baker McKenzie – Юридичний радник; Юлія Бадрітдінова, McDonald's; Василь Бовділов, Unilever; Василе Варварой, Cargill; Тарас Панасенко, Avrora Multimarket; Леонід Полупан, Microsoft; Петро Рондяк, Winner Group; Анджей Ружицький, Bunge; Олена Середа, Coca-Cola; Олег Хайдакін, Carlsberg; Михайло Харенко, Sayenko Kharenko; Андрій Цимбал, KPMG.

Президент: Андрій Гундер

Додаток до листа Американської торгівельної палати в Україні
№ 25 – 16 від 16 січня 2025 року

Пропозиції експертів компаній-членів Палати до проекту Закону №12207 «Про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки»

1. Виникають сумніви щодо доцільності створення нового регуляторного (контролюючого) органу – центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері кібербезпеки, в період дії воєнного стану та/або у післявоєнний період, а також джерел його фінансування та забезпечення.

Вказаний законопроект розроблений з метою імплементації в національне законодавство положень Директиви Європейського Союзу (далі – ЄС) від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на території Союзу, внесення змін до Регламенту (ЄС) 910/2014 і Директиви (ЄС) 2018/1972, а також про скасування Директиви (ЄС) 2016/1148 (NIS 2) (далі – Директива).

Водночас, ст. 8 Директиви встановлює, що кожна держава-член ЄС призначає або створює один або кілька компетентних органів, відповідальних за кібербезпеку та виконання завдань нагляду, зазначених у Главі VII (компетентні органи). Україні це дозволяє виконати вимоги Директиви із врахуванням національної системи кібербезпеки в Україні з відповідним уточненням повноважень основних суб'єктів цієї системи та належним розподілом завдань в цій сфері.

Крім того, в законопроекті запропоновано модель державного управління, що передбачає виконання функції та завдань у сфері кібербезпеки та захисту інформації різними органами державної влади, що є не достатньо обґрунтованим з огляду на те, що ці домени управління є пов'язаними в загальній системі управління інформаційною безпекою, та враховуючи поточні заходи оптимізації бюджетних витрат.

2. На думку експертів компаній-членів Палати, окремі положення законопроекту передбачають необмежену дискрецію регуляторного органу та невідповідність базовим принципам побудови національної системи органів виконавчої влади.

У разі реалізації запропонованого проектом підходу на центральний орган виконавчої влади покладатиметься здійснення одночасно і правовстановлюючих, і правореалізаційних, і контролюючих повноважень. Таким чином, на зазначений орган публічної влади, по суті, покладатиметься самостійне визначення правил власної діяльності, своїх прав та обов'язків, що не може бути підтримане та містить ознаки надмірної дискреції у повноваженнях.

Також, законопроектом необґрунтовано та без врахування національної системи кібербезпеки, пропонується наділити Національну комісію з цінних паперів та фондового ринку України окремими повноваженнями встановлювати вимоги кіберзахисту та здійснювати заходи контролю за їх виконанням щодо суб'єктів господарювання, які здійснюють види професійної діяльності на ринках капіталу та організованих товарних ринках.

3. Окремі положення законопроекту не відповідають чинним міжнародним стандартам.

Законопроектом передбачаються адміністративно-господарські санкції у вигляді надвисоких штрафів, аналогів яким немає у вітчизняному законодавстві.

Водночас, відповідно до зазначеної вище Директиви, примусові заходи, у тому числі адміністративні штрафи, мають бути пропорційними, а їх накладення повинно підлягати належним процесуальним гарантіям відповідно до загальних принципів права ЄС та Хартії основних прав ЄС, включаючи право на ефективний засіб правового захисту та справедливий суд, презумпцію невинуватості та захист.

Застосування штрафних санкцій в законодавстві України так само є інструментом попередження вчинення правопорушення, а не інструментом тиску. Зазначена позиція також була висловлена Головним науково-експертним управлінням Апарату Верховної Ради України у науково-експертному висновку щодо законопроекту.

ПРИЗНАЧЕНО ДЛЯ ВКАЗАНИХ АДРЕСАТІВ, НЕ ДЛЯ ПУБЛІЧНОГО РОЗПОВСЮДЖЕННЯ

Тому, на думку експертів компаній-членів Палати, доцільним є застосування підходу, коли за вчинення незначного порушення вперше має застосовуватись попередження та інструкція щодо коригування дій. В подальшому штрафи будуть застосовуватись, проте їх розмір повинен бути суттєво зменшений з огляду на нестабільну економічну ситуацію та дію воєнного стану.

4. Існують сумніви щодо належної продуманості запропонованої в законопроекті імплементації європейської схеми сертифікації.

Законопроект фактично запроваджує обов'язкову сертифікацію продуктів інформаційно-комунікаційних технологій (далі – ІКТ), послуг ІКТ та процесів ІКТ. Водночас Директива (ЄС) 2022/2555 та Регламент (ЄС) 2019/881 безпосередньо не встановлюють такої обов'язкової сертифікації. Враховуючи положення цих актів ЄС вимоги щодо використання сертифікованих продуктів ІКТ, послуг ІКТ та процесів ІКТ, на думку експертів компаній-членів Палати, має відбуватися з урахуванням ризик-орієнтованого підходу, який враховує потенційні загрози та специфіку діяльності певних користувачів, зокрема у певних секторах.

Крім того, Регламент (ЄС) 2019/881 не обмежується лише схемою сертифікації на основі критеріїв European Common Criteria (далі – EUCC). Регламент (ЄС) 2019/881 дозволяє створення нових спеціалізованих схем сертифікації для конкретних категорій ІКТ-продуктів, послуг чи процесів, які можуть не підпадати під схему сертифікації на основі критеріїв EUCC. Наприклад, це можуть бути схеми, запроваджені для сертифікації хмарних послуг, безпеки 5G, штучного інтелекту тощо. Отже, законопроект з одного боку визнає європейські схеми сертифікації, а з іншого – звужує їх сферу, що, на погляд експертів компаній-членів Палати, є дещо непослідовним підходом, якщо метою законопроекту є імплементація до українського законодавства положень Директиви (ЄС) 2022/2555 та Регламенту (ЄС) 2019/881.

5. Виникають сумніви щодо нагальності та пріоритетності імплементації положень Директиви в українське законодавство.

Слід зазначити, що Директива ЄС (ЄС) 2022/2555 набула чинності 16 січня 2023 року, а окремі організаційні заходи мають бути виконані державами-членами до квітня 2025 року.

Відповідно, наразі відсутня правозастосовча практика реалізації положень Директиви самими країнами-членами ЄС. Відсутність єдиної узгодженої позиції щодо способів виконання вимог Директиви серед самих країн-членів може також ускладнити адаптацію її положень до українських реалій.

6. Законопроект містить низький рівень змістовного наповнення відповідно до вимог нормопроєктувальної техніки, наявність стилістичних та орфографічних помилок, неузгодженості або дублювання норм законопроекту з чинними законами України, а також вживання термінів та понять, які не уніфіковані в усьому його тексті (без використання синонімів та словосполучень, що мають подібне лексичне значення) та термінологією *acquis* ЄС, що потенційно ускладнюватиме подальше правозастосування.