ІНТЕРНЕТ АСОЦІАЦІЯ УКРАЇНИ
04053, м. Київ, вул. О.Гончара, 15/3, офіс 22
info@inau.ua; www.inau.ua

Голові Комітету Верховної Ради України з питань цифрової трансформації КРЯЧКУ М.В.

Вих. № 108/1
від 19.12.2024

Щодо проекту Закону № 12207 від 14.11.2024

Шановний Михайле Валерійовичу!

Інтернет Асоціація України (ІнАУ), яка об'єднує понад 220 підприємств галузі інформаційно-комунікаційних технологій, висловлює Вам свою повагу та звертається з наступним.

14 листопада 2024 року у Верховній Раді України за №12207 зареєстровано проект Закону про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки (далі – проект Закону №12207). За результатом аналізу цього документу надаємо зауваження та пропозиції, які просимо розглянути та врахувати.

1. Надмірне регулювання малого бізнесу у сфері кіберзахисту суперечить європейському підходу і матиме зворотній - руйнівний ефект для кібербезпеки.

Пояснювальна записка до проекту Закону України №12207 єдиною метою його прийняття зазначає необхідність імплементації до українського законодавства положень Директиви (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на території Союзу (далі – Директива ЄС №2022/2555). Ознайомитись з цією Директивою можна за посиланням https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555.

Мусимо зазначити, що хоча проект Закону №12207 і містить цілий ряд норм, прямо перекладених з Директиви ЄС №2022/2555, в частині підходів до регулювання малого бізнесу у сфері кіберзахисту він суттєво відрізняється від Директиви і суперечить її нормам: ***проект Закону №12207 містить значно більш жорсткі норми регулювання підприємств малого бізнесу у сфері кіберзахисту, ніж передбачає Директива ЄС №2022/2555***.

Зокрема, в ст.3 Директиви ЄС №2022/2555 суб'єктами з високою критичністю (essential) вважаються серед іншого такі суб'єкти господарювання:

- постачальники публічних електронних комунікаційних мереж або послуг, які кваліфікуються як ***середні*** підприємства;
- визначені в Додатку I Директиви ЄС №2022/2555 суб'єкти (в тому числі точки обміну трафіком), які перевищують рівні для ***середніх*** підприємств.

Отже, постачальники публічних електронних комунікаційних мереж або послуг і точки обміну трафіком, які не є середніми і кваліфікуються як малі та мікро підприємства, Директивою ЄС №2022/2555 не відносяться до суб'єктів господарювання з високою критичністю (essential), а відносяться в плані кібербезпеки лише до інших важливих (important) суб'єктів господарювання.

А проект Закону №12207 – навпаки, всупереч Директиві ЄС №2022/2555, такі мікро- і малі підприємства відносить до суб'єктів господарювання з високою критичністю з відповідними максимальними вимогами щодо кібезбезпеки.

Ці максимальні вимоги щодо кібербезпеки дуже складні до виконання малим бізнесом (що розуміють в Євросоюзі), отже, існує високий ризик, що такі підприємства в разі прийняття проекту Закону №12207 будуть ліквідовані в Україні або самими власниками в очікуванні штрафів, або за підсумками перевірки і сплати таких штрафів.

Важливо, що велика кількість постачальників послуг електронних комунікацій сама по собі є фактором кібербезпеки держави, а вихід з ринку підприємств малого бізнесу погіршить національну безпеку і сталість інтернет-мереж, адже кібератаки і підкуп персоналу з метою знищення систем управління мережами електронних комунікацій найбільш ефективні щодо малої кількості крупних гравців, ніж до значної кількості малих (що показав нещодавній досвід кібератак на крупних українських операторів).

При цьому авторами проекту Закону №12207 взагалі не згадуються великі підприємства в контексті забезпечення ними кібербезпеки: до категорії «суб'єкт виконання вимог з кібербезпеки» пропонується віднести суб'єктів господарювання будь-якої форми власності, які належать до категорії ***середніх підприємств*** відповідно до Закону України «Про бухгалтерський облік та фінансову звітність в Україні» та здійснюють свою діяльність у секторах з високою критичністю та інших критичних секторах, в той час, як ***категорія «великих підприємств», вказана у цьому ж Законі, не вважається «суб'єктом виконання вимог з кібербезпеки».***

З іншого боку, проект Закону №12204 пропонує ***віднесення фізичних осіб*** до суб'єктів виконання вимог з кібербезпеки. Не вважається зрозумілим та юридично можливим встановлення однакових вимог та здійснення однакового контролю за виконанням цих вимог з кібербезпеки абсолютно всіма особами (громадянами і негромадянами) на території України. Відтак, вважаємо, що така пропозиція містить корупційні ризики, коли контролюючий орган на власний розсуд матиме право вибіркового контролю за людьми, здійснення перевірок та притягнення їх до відповідальності.

Отже, спрямування проекту Закону №12207 на регулювання кібербезпеки мікро- і малого бізнесу і, навіть, фізичних осіб, при одночасній відсутності навіть згадок про великі підприємства, суперечить не лише нормам Директиви ЄС №2022/2555, але й нормальній логіці.

2. Створення ще одного додаткового державного органу у сфері кібербезпеки призведе до збільшення бюрократії і не покращить кібербезпеку.

Директива ЄС №2022/2555 не вимагає створення додаткових органів з питань кібербезпеки, а лише визначає, що кожна держава-член ЄС призначає або створює один або кілька компетентних органів, відповідальних за управління масштабними інцидентами та кризами кібербезпеки (органи управління кіберкризовими ситуаціями).

В Україні вже створено не один, а цілий ряд державних органів, які опікуються державною політикою у сфері кібербезпеки і кіберкризовими ситуаціями (не рахуючи МЗС, МО, ГШ ЗСУ, розвідувальні і прикордонні органи, які мають підрозділи з питань кібербезпеки):

- Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку);
- Міністерство цифрової трансформації;
- Національний координаційний центр кібербезпеки (НКЦК);
- Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України (ДКІБ СБУ);
- Департамент кіберполіції Національної поліції України;
- Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

А ***проект Закону №12207 пропонує створення ще одного нового органу - центрального органу виконавчої влади, що має забезпечувати формування та реалізацію державної політики у сфері кібербезпеки.***

Вважаємо, що нагальною потребою української держави, особливо у надзвичайно важких умовах війни і бюджетного та кадрового дефіциту, є значне скорочення існуючих державних структур. З метою економії коштів платників податків і скорочення державного апарату всі функції з питань кібербезпеки, крім військових, доцільно зосередити в одному органі - Міністерстві цифрової трансформації або Держспецзв'язку, які і сьогодні виконують функції з формування та реалізації державної політики у сфері кібербезпеки. ***Множення державних органів та передача між ними функцій в сьогоднішніх умовах не лише збільшить навантаження на бюджет, а й створить додаткові ризики для забезпечення кібербезпеки держави у перехідний період.***

Отже, пропоноване ***проектом Закону №12207 створення ще одного Центрального органу виконавчої влади у сфері кібербезпеки вважаємо не лише неактуальним, але й шкідливим для кібербезпеки держави.***

У разі, якщо законодавець все ж вважає доцільним створення єдиного органу виконавчої влади для забезпечення формування та реалізації державної політики у сфері кібербезпеки, то це має відбуватись з обов'язковою ліквідацією інших дублюючих органів у цій сфері, здійснюватись у мирний час, при наявності достатніх кадрових ресурсів і вільних коштів державного бюджету.

3. Проект Закону №12207 порушує принципи мінімально необхідного регулювання і суперечить цілому ряду норм законодавства України.

Ст.2 Закону України «Про основні засади забезпечення кібербезпеки України» визначає принципи застосування Закону у цій сфері, серед них: мінімально необхідне регулювання, збалансованість вимог та відповідальності, недискримінація, еквівалентність.

Вважаємо, що в разі прийняття проекту Закону №12207, зазначені принципи мінімально необхідного регулювання будуть порушені з огляду на таке:

- ***неточність і розпливчатість формулювань*** проекту Закону №12207, а також наявність у ньому оціночних понять, які можуть довільно тлумачитись контролюючими органами, створюють ситуацію невизначеності для суб'єкта виконання вимог з кібербезпеки, і, відповідно, несуть корупційні ризики;

- проект Закону №12207 встановлює ***неадекватно високі розміри штрафів*** – від 7 млн грн лише за неподання, неповне подання або за порушення строків подання інформації на запит уповноваженого органу у сфері кібербезпеки, що загрожує самому існуванню суб'єкта господарювання, а для підприємств мікробізнесу такий штраф співрозмірний з їх балансовою вартістю, що безумовно призведе до банкрутства і ліквідації такого підприємства; такий підхід є незбалансованим і дискримінаційним щодо підприємств мікро- і малого бізнесу;

- проект Закону №12207 пропонує застосування адміністративно-господарських санкцій (штрафів) не лише до суб'єктів господарювання, а і ***до посадових осіб***, що є неприпустимим і суперечить ст. 238, 241 Господарського кодексу України;

- проект Закону №12207 передбачає ***повну матеріальну відповідальність посадових осіб*** суб'єкта виконання вимог з кібербезпеки за шкоду, завдану суб'єкту виконання вимог з кібербезпеки, що прямо суперечить статті 134 та іншим статтям Глави IX КЗпП України, якою врегульовано випадки повної матеріальної відповідальності;

- проект Закону №12207 ***не передбачає жодної відповідальності посадових осіб центрального органу виконавчої влади у сфері кібербезпеки та інших державних органів***, які допустили порушення прав суб'єктів господарювання або нанесли їм шкоду своїми

незаконними діями при здійсненні повноважень, що порушує принципи збалансованості вимог, відповідальності та еквівалентності;

- положеннями щодо негласних перевірок у проекті Закону створюються умови для ***безпідставного, протизаконного притягнення до відповідальності суб'єктів*** виконання вимог з кібербезпеки та їх посадових осіб;

- моніторинг ланцюга постачання, включно з перевіркою безпеки відносин між кожним суб'єктом та його прямими постачальниками або суб'єктами виконання вимог з кібербезпеки, моніторингу безпеки в придбанні, розробці та обслуговуванні послуг електронних комунікаційних мереж та інформаційних систем, ***суперечить вимогам Господарського кодексу України,*** який визначає, що суб'єкти господарювання мають право без обмежень самостійно здійснювати господарську діяльність; доречніше визначити перелік постачальників, товарів, робіт і послуг, які не мають використовуватись суб'єктами виконання вимог з кібербезпеки;

- проект Закону №12207 містить цілий ряд інших невідповідностей діючому законодавству України.

Деталі щодо невідповідностей норм проекту Закону №12207 діючому законодавству України – у додатку.

З урахуванням наведеного, вважаємо, що текст проекту Закону потребує суттєвого доопрацювання і його прийняття у запропонованій редакції є недоцільним. Тому, **просимо за результатом розгляду проекту Закону у Вашому Комітеті, рекомендувати повернути проект Закону на доопрацювання без його включення до порядку денного та розгляду на пленарному засіданні Верховної Ради України.**

Про результати розгляду цього листа просимо повідомити письмово.

Додаток: Невідповідності норм проекту Закону №12207 чинному законодавству України на 7 арк.

З повагою

Голова Правління
ІНТЕРНЕТ АСОЦІАЦІЇ УКРАЇНИ **Олександр САВЧУК**