Додаток до листа ІнАУ від 19.12.2024 № 108/1-6

НЕВІДПОВІДНОСТІ НОРМ ПРОЕКТУ ЗАКОНУ №12207 ЧИННОМУ ЗАКОНОДАВСТВУ УКРАЇНИ

Щодо змін до Закону України «Про основні засади забезпечення кібербезпеки України».

1. У пункті 31 статті 1 змін до Закону України «Про основні засади забезпечення кібербезпеки України» пропонується таке визначення поняття: «оператор послуг з реєстрації доменних імен (DNS) – юридична особа, яка надає: ***загальнодоступні послуги рекурсивного визначення доменних імен*** для ***кінцевих користувачів Інтернету***; або авторизовані послуги з визначення доменних імен (комплекс заходів з утворення запису про доменне ім'я і та надання прав використання доменного імені) для використання третіми особами, за винятком серверів кореневих імен».

Разом з цим, у проекті Закону не розкрито поняття, що таке «загальнодоступні послуги рекурсивного визначення доменних імен», хто є «кінцевими користувачами Інтернету». Тому, визначення поняття «оператор послуг з реєстрації доменних імен (DNS) є нечітким та може мати різне його розуміння при застосуванні.

2. У пункті 41 статті 1 змін до Закону України «Про основні засади забезпечення кібербезпеки України» до суб'єктів виконання вимог з кібербезпеки пропонується віднести ***фізичну*** або юридичну ***особу***, у тому числі суб'єкт владних повноважень, ідентифікований в порядку, визначеному цим Законом як суб'єкт, на якого цим Законом покладено виконання та забезпечення виконання вимог з кібербезпеки.

2.1. Разом з цим видається сумнівним правомірність віднесення *фізичних осіб* до суб'єктів виконання вимог з кібербезпеки. У законодавстві України, зокрема, у статті 24 ЦК України надано поняття «фізичної особи», а саме, «людина як учасник цивільних відносин» вважається фізичною особою. Тому, не вважається зрозумілим та юридично можливим встановлення вимог та здійснення абсолютно однакового контролю за виконанням вимог з кібербезпеки абсолютно всіма людьми (громадянами і негромадянами) на території України. Відтак, вважаємо, що запропоноване визначення містить корупційні ризики, коли контролюючий орган на власний розсуд матиме право вибіркового контролю за людьми, здійснення перевірок та притягнення їх до відповідальності.

2.2. У визначенні цього терміну також застосовується поняття ***«загальнодоступні електронні комунікаційні послуги***». Проте, таких послуг, з втратою чинності Законом України «Про телекомунікації» з 01.01.2022, не існує. Застосовується поняття «універсальна електронна комунікаційна послуга». Крім того, не зрозуміло, які критерії впливають на те, щоб усі постачальники цих послуг «автоматично» були віднесені до категорії «суб'єкт виконання вимог з кібербезпеки».

2.3. Також не зрозуміло, з яких причин 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 буде вважатись «суб'єктом виконання вимог з кібербезпеки».

Таким чином, пункт 41 статті 1, а також стаття 5^4 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» підлягає суттєвому доопрацюванню з метою віднесення до категорії «суб'єкти виконання вимог з кібербезпеки» виключно юридичних осіб і лише насправді важливих галузей економіки.

3. У пункті 44 статті 1 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» пропонується визначення терміну «***системи електронних комунікацій***», яке, як на наш погляд, не узгоджується із термінами «електронна комунікація», «електронна комунікаційна мережа», «технічні засоби електронних комунікацій», наданими у спеціальному законі – Законі України «Про електронні комунікації».

4. У пункті 13 частини третьої статті 5^1 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» центральному органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері кібербезпеки (далі - уповноважений орган), пропонується надати повноваження ***затверджувати вимоги до методики проведення моніторингу безпеки 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***, включаючи врегулювання вразливостей та розкриття інформації, закупівлі устаткування, обладнання, технічних засобів, продуктів ІКТ, послуг ІКТ або процесів ІКТ.

Пропонуємо це положення виключити із проекту Закону, оскільки невідомо, за рахунок яких людських ресурсів, в першу чергу, це положення реалізовуватиметься. Взагалі не зрозуміло, який обсяг повноважень та знань повинен мати перевіряючий для того, щоб кваліфіковано реалізувати ці повноваження та визначати вимоги до методики проведення моніторингу. Відповідно до частини першої статті 19 Господарського кодексу України суб'єкти господарювання мають право без обмежень самостійно здійснювати господарську діяльність, що не суперечить законодавству. У частині третій статті 19 Господарського кодексу України чітко встановлено сфери, у яких держава здійснює контроль і нагляд за господарською діяльністю суб'єктів господарювання. Також частинами п'ятою-шостою статті 19 згаданого кодексу визначено, незаконне втручання та перешкоджання господарській діяльності суб'єктів господарювання з боку органів державної влади, їх посадових осіб при здійсненні ними державного контролю та нагляду **забороняються.** Органи державної влади і посадові особи зобов'язані здійснювати інспектування та перевірки діяльності суб'єктів господарювання неупереджено, об'єктивно і оперативно, дотримуючись вимог законодавства, поважаючи права і законні інтереси суб'єктів господарювання. Тому, вважаємо, згадане положення у проекті Закону, містить ознаки втручання в господарську діяльність, що заборонено законодавством та, фактичної результативності не матиме у практичному застосуванні, окрім, як безкінечних запитів та перевірок уповноваженого органу. Доречно було б визначити лише, що саме, тобто, які товари, роботи і послуги, і від яких постачальників, в т.ч. в ланцюгу постачання/отримання, суб'єкти виконання вимог з кібербезпеки не повинні придбавати/отримувати тощо та, відповідно, здійснювати державний контроль за цим.

5. У частині шостій статті 5^1, зокрема, підпунктах 1 та 2, проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» пропонується встановити, що суб'єкти виконання вимог з кібербезпеки надають уповноваженому органу інформацію, ***необхідну для оцінювання*** безпеки електронної комунікаційної мережі, електронної комунікаційної послуги та

інформаційних систем, у тому числі документально встановленої політики безпеки; усувають ***будь-яку невідповідність*** вимогам, затвердженим уповноваженим органом. Вважаємо, що ці положення проекту Закону є не точними, адже чітко не встановлено порядок та процедури надання такої інформації до уповноваженого органу, принаймні, орієнтовний перелік питань, з яких може запитуватись інформація, що таке «будь-яка невідповідність» і т.д.

6. У пункті 3 частини третьої статті 8 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» пропонується надати Службі безпеки України повноваження ***негласних перевірок готовності*** операторів критичної інфраструктури до можливих кібератак та кіберінцидентів. Проте, з метою недопущення зловживання владою та повноваженнями, повинні бути затверджені певні інструкції щодо порядків та процедур реалізації таких повноважень, а також перелік вичерпного кола прав перевіряючого. Крім того, не зрозуміла взагалі мета таких повноважень. Було б достатньо на законодавчому рівні розробити чіткі та зрозумілі заходи у сфері кібербезпеки та такі ж чіткі, прозорі та зрозумілі процедури державного нагляду (контролю) за їх виконанням. Адже статтею 19 Конституції України гарантовано, що правовий порядок в Україні ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбачено законодавством. Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. Проте, вказаними вище положеннями у проекті Закону створюються умови для безпідставного, протизаконного притягнення до відповідальності суб'єктів виконання вимог з кібербезпеки та їх посадових осіб.

7. У статті 12 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» регулюються питання ***відповідальності*** за порушення законодавства у сфері кібербезпеки. В першу чергу, звертаємо увагу, що положення цієї статті є нечіткими, невизначеними, містять неодноразові повтори «будь-які», замість встановлення чіткого переліку обставин, які враховуватиме суб'єкт застосування заходів впливу.

8. Стаття 16, зокрема, частина одинадцята, проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України», якою пропонується регулювати умови застосування продуктів ІКТ, послуг ІКТ та процесів ІКТ, також є нечіткою. Положення цієї статті закону надаватимуть право уповноваженому органу, за наявності ***обґрунтованих сумнівів*** у відповідності проведеної процедури оцінки відповідності вимогам законодавства, можливість подати запит до органу з оцінки відповідності про надання аудиторського звіту щодо проведення процедури оцінки відповідності вимогам кібербезпеки для підтвердження того, що він відповідає вимогам сертифікації кібербезпеки. Тобто, що таке «обґрунтовані сумніви»? Це звичайна суб'єктивна оцінка певної ситуації уповноваженим органом, яка не ґрунтуватиметься на нормах законодавства. Встановлення таких дискреційних повноважень уповноваженого органу у законі вважаємо неприпустимим.

9. У статті 18 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» висвітлено положення про здійснення державного нагляду (контролю) у сфері кібербезпеки та зазначено, що такий нагляд здійснюватиметься уповноваженим органом відповідно до принципів і порядку здійснення державного нагляду (контролю) встановлених у Законі України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності». Разом з цим, у цьому Законі, немає такої форми здійснення

державного нагляду (контролю), як-то ***безвиїзний нагляд***. Також, з тексту проекту Закону не зрозуміло, що таке ***«сканування безпеки», «спеціальний аудит» тощо.***

Як вид позапланової перевірки пропонуються і ***перевірки на місці та нагляд***, ***вибіркові перевірки***, які проводяться експертами з кібербезпеки. Таке положення потребує однозначного виключення із тексту проекту Закону, оскільки ані в тексті проекту Закону, ані в чинних законодавчих актах не розкриті такі поняття, порядки та процедури їх проведення. А надання уповноваженому органу право здійснювати вибіркові перевірки без встановлення будь-яких критеріїв та підстав для перевірки, вважаємо, містить корупційну складову, необмежене право здійснювати перевірки безпідставно.

Таким чином, порядок і процедура здійснення державного нагляду (контролю) уповноваженим органом, яка запропонована у статті 18 не відповідає Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності».

10. У статті 20 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» наведено заходи впливу та реагування, які застосовуються до суб'єкта виконання вимог з кібербезпеки за порушення законодавства у сфері кібербезпеки.

10.1. Зокрема, у частині першій цієї статті пропонується, у разі невиконання (неналежного виконання) суб'єктом виконання вимог з кібербезпеки ***(його посадовою особою***) вимог законодавства у сфері кібербезпеки, ***до нього адекватно вчиненому порушенню*** протягом шести місяців з дня виявлення порушення, але не пізніше ніж через три роки з дня його вчинення, застосовуються такі заходи впливу та реагування.

Проте, що таке визначення заходу впливу та реагування «адекватно вчиненому порушенню»? Ані в Господарському кодексі України, ані в інших законодавчих актах, які в тій чи іншій мірі регулюють питання реагування суб'єктів владних повноважень на виявлення та припинення порушень у певній сфері діяльності чи застосування адміністративно-господарських санкцій (штрафу), таке поняття не розкривається. Тобто, положенням проекту Закону пропонується, щоб таку «адекватність» на власний розсуд оцінювали працівники уповноваженого органу. Проте, окрім того, що така ініціатива є нечіткою та невизначено, вона є непрозорою, що матиме наслідком необмежені можливості зловживання працівниками уповноваженого органу у ході реалізації своїх владних повноважень.

10.2. Відповідно до статей 238, 241 Господарського кодексу України адміністративно-господарські санкції застосовуються до суб'єктів господарювання. Разом з цим у частині першій статті 20 змін до Закону України «Про основні засади забезпечення кібербезпеки України» положення («*до нього*») сформоване таким чином, що складається враження, що адміністративно-господарські санкції (штраф) будуть застосовуватись і до посадових осіб, що є неприпустимим.

10.3. Також чітко не вказано, у яких випадках уповноважений орган може застосувати до порушника встановлення якоїсь із вимог, перелік яких наведено у пунктах 1-3 частини першої статті 20 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України», а у яких випадках застосовуватиметься адміністративно-господарська санкція (штраф). Тобто, вважаємо, що це положення містить корупційні ризики, у разі його практичного застосування.

10.4. У частині третій статті 20 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» наведено розміри штрафів, які можуть застосовуватись до суб'єкта виконання вимог з кібербезпеки. Розміри таких штрафів запропоновано

визначати у мільйонах гривень, або застосовувати у розмірах, які обраховуватимуться у відсотках від загального річного обороту суб'єкта виконання вимог з кібербезпеки.

З цього приводу слід зазначити, що, по-перше, у запропонованих законодавчих положеннях чітко не визначено, коли штраф застосовуватиметься у сталій сумі, а у яких випадках із розрахунку від загального річного обороту. Відсутність такого розмежування саме у Законі створить корупційні ризики та несправедливе застосування штрафів до суб'єктів виконання вимог з кібербезпеки у разі вчинення однакових порушень, проте штрафи до різних суб'єктів можуть бути різними. У Пояснювальній записці до проекту Закону відсутні пояснення стосовно пропозицій, як на наше переконання, занадто високих розмірів штрафів, проте, здається, чинне законодавство ще не містить норм, які надавали б право застосовувати розміри штрафів, які обраховуються мільйонами, а тим більше, за «інформаційні порушення», як-то неподання або подання не в повному обсязі інформації та/або документів тощо. До того ж, не зрозуміло, яке відношення до порушення виконання вимог з кібербезпеки має загальний річний оборот суб'єкта господарювання і чому саме від цього показника запропоновано здійснювати розрахунок, а не виходячи, наприклад, із неоподатковуваних мінімумів доходів громадян.

10.5. У частині дев'ятій статті 20 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» пропонується встановити, що ***посадова особа*** суб'єкта виконання вимог з кібербезпеки, на яку відповідно до законодавства, статуту або внутрішніх документів суб'єкта виконання вимог з кібербезпеки, покладено обов'язки щодо дотримання вимог у сфері кібербезпеки, визначених цим Законом, ***несе повну матеріальну відповідальність за шкоду, завдану суб'єкту*** виконання вимог з кібербезпеки, у зв'язку із застосуванням до нього заходу впливу у вигляді штрафу з підстав, визначених цим Законом, крім випадків, коли вона доведе відсутність своєї вини у вчиненні порушення, яке стало підставою для застосування такого заходу впливу.

Тобто, за непрозорих умов та процедур накладення штрафів на суб'єктів виконання вимог з кібербезпеки у проекті Закону запропоновано, що такі штрафи повинні компенсуватись фізичними особами – посадовими особами такого суб'єкта.

Відповідно до статей 238, 241 Господарського кодексу України адміністративно-господарські санкції застосовуються до суб'єктів господарювання, а не до посадових осіб. Крім того, жодним нормативно-правовим актом не встановлено такої обтяжливої вимоги до посадової особи суб'єкта господарювання, по суті, відшкодування багатомільйонних штрафів. До того ж, вказане положення у проекті Закону прямо суперечить статті 134 та іншим статтям Глави IX КЗпП України, якими врегульовано випадки повної матеріальної відповідальності. У ієрархії законодавчих актів кодекс має вищу юридичну силу аніж закон.

10.6. У частині одинадцятій статті 20 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» зазначено, що *рішення уповноваженого органу про застосування заходів впливу може бути оскаржено до суду.*

Проте, строки оскарження таких рішень, порядок та процедури не розкриті.

Таким чином, в цілому, у запропонованій статті проекту Закону нечітко визначені вид, умови та підстави відповідальності суб'єктів виконання вимог з кібербезпеки, що, на наше переконання, взагалі унеможливлює практичне застосування цієї статті.

З огляду на зазначене, стаття 20 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» потребує суттєвого доопрацювання, з огляду як на значні юридичні недоліки, встановлені дискреційні повноваження уповноваженого органу та,

відповідно, корупційні ризики, а також вкрай негативні наслідки від застосування адміністративно-господарських санкцій у занадто значних розмірах на суб'єктів господарювання та людей - посадових осіб.

11. У проекті Додатку 1 до Закону України «Про основні засади забезпечення кібербезпеки України» запропоновано перелік секторів з критичною важливістю. Згідно з положеннями законодавства у сфері кібербезпеки, що застосовується на сьогодні, перелік таких секторів затверджується Кабінетом Міністрів України. Вважаємо, що нині існуючий спосіб є більш прийнятним для застосування, зокрема, в умовах воєнного стану в Україні, адже, за потреби, внести певні зміни до постанови Кабінету Міністрів України значно швидше в часі, аніж внести зміни у закон. Також, у секторі «8. Цифрова інфраструктура» застосовуються типи суб'єктів, визначення яких не надано в українському законодавстві, або ці визначення у секторі зазначені неправильно (не у відповідності до термінів Закону України «Про електронні комунікації»), як-то: «постачальники електронних комунікаційних мереж *загального користування*», «постачальники електронних комунікаційних послуг *загального користування*».

12. По тексту проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» вживаються положення, застосування яких може містити корупційні ризики. До прикладу, у визначенні терміну «рівень надійності» застосовується поняття «***основа впевненості***», проте, що складає таку основу впевненості невідомо. Тобто, застосування цього законодавчого припису надаватиме право контролюючим органам визначати таку «основу впевненості» на власний розсуд, суб'єктивно.

У частині четвертій статті 5^4 проекту змін до Закону України «Про основні засади забезпечення кібербезпеки України» зазначено, що «суб'єкти виконання вимог з кібербезпеки вживають ***пропорційні технічні та організаційні*** заходи для управління ризиками безпеки електронної комунікаційної мережі та/або послуги, інформаційних систем, інформаційно-комунікаційних систем, які використовуються для надання послуг.» Проте, Закон має містити чіткий перелік таких заходів, який би був прозорим та зрозумілим як для суб'єктів виконання вимог з кібербезпеки, так і для контролюючих органів. А що таке «пропорційні технічні та організаційні» і коли вжиття таких заходів є достатнім, в проекті Закону не прописується.

Тобто, у проекті Закону, як в наведених прикладах, так і в цілому по тексту, застосовуються оціночні поняття, які можуть довільно тлумачитись контролюючими органами з корупційною метою.

Також у проекті змін до Закону України «Про основні засади забезпечення кібербезпеки України» немає чіткого та зрозумілого підходу до визначення кола суб'єктів, яких стосуватиметься виконання положень цього Закону.

13. Значна частина пропозицій змін до Закону України «Про основні засади забезпечення кібербезпеки України» стосується зміни та введення нових термінів у законодавство у сфері кібербезпеки. Проте, термінологія у проекті Закону потребує суттєвого доопрацювання на предмет створення чітких, зрозумілих та однозначних формулювань для їх практичного застосування з метою непорушення принципу правової визначеності й недопущення неправильного трактування та правозастосування.

<u>Щодо змін до Закону України «Про національну безпеку України».</u>

1. У пропозиціях доповнити підпунктом 14-1 статтю 1 Закону України «Про національну безпеку України» застосовуються поняття «***ландшафт кіберзагроз***», «***потенціал кібербезпеки***». Проте, що це, далі не розкрито, відтак не зрозуміло, як практично ці поняття будуть застосовуватись. Що таке «***оцінка загального рівня обізнаності щодо кібербезпеки***…», «***сукупна оцінка результатів експертних перевірок***» та «***сукупна оцінка рівня розвиненості потенціалів і ресурсів кібербезпеки в державі***», тобто, які критерії та шкала для такої оцінки та як здійснюватимуться сукупні оцінки, взагалі, що таке «сукупна оцінка» у розумінні тесту цього проекту Закону та українського законодавства, що регулює питання кібербезпеки?

2. Змінами пункту 4 частини третьої статті 27 Закону України «Про національну безпеку України» пропонується встановити, що Кабінет Міністрів України визначає порядок проведення ***огляду стану*** *забезпечення кібербезпеки*, - центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері кібербезпеки. Проте, чинна редакція цього законодавчого положення є точнішою та зрозумілішою, адже чітко визначає, що такий огляд стану кіберзахисту стосується лише таких об'єктів, як критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Щодо змін до Закону України «Про електронні комунікації».

1. Визначення терміну «***електронна комунікаційна мережа***» пропонуємо залишити без змін, оскільки, вважаємо, що цей термін не стосується мети, з якою розроблено проект Закону, та, в цілому не відповідатиме застосуванню цього терміну у Законі України «Про електронні комунікації». Крім цього, у запропонованому у проекті визначенні терміну застосовуються поняття, яких, на сьогодні не існує у національному законодавстві, як-то «мережі кабельного телебачення», «телевізійне мовлення». У Законі України «Про електронні комунікації» не застосовуються й такі поняття, як-то «дротові, радіо-, оптичні або інші електромагнітні засоби», «електросилові кабельні системи».

2. Пропозицію доповнити статтю 3 Закону України «Про електронні комунікації» частиною третьою, виключити, оскільки ці пропозиції не стосуються предмету цього Закону, а можуть бути положеннями законодавства у сфері кібербезпеки. Відповідно до пунктів 2.2 та 2.3 розділу 2 Правил оформлення проектів законів та основні вимоги законодавчої техніки (Методичні рекомендації) текст законопроекту має викладатися стисло, державною діловою мовою, за змогою, короткими фразами. Не варто застосовувати вислови з багатьма підрядними реченнями. Особливу увагу необхідно звертати на точність термінології. Нормативні положення закону не повинні містити зайвої деталізації. Потрібно завжди пам'ятати, що закон регулює суспільні відносини, а не вирішує конкретне питання для конкретної фізичної чи юридичної особи. Мова викладення нормативного матеріалу має бути чітка та однозначна. Зазвичай одне речення повинно містити одну правову норму. Вважаємо, що саме ці положення Методичних рекомендацій не враховані у тексті проекту Закону.