Додаток

ПРОПОЗИЦІЇ ТА ЗАУВАЖЕННЯ

до проекту Закону України про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки (реєстр. № 12207 від 14.11.2024)

1. У Законі України "Про основні засади забезпечення кібербезпеки України":

1) стаття 1:

у пункті 2 замість слів "**безпека**" і "**дія**" вжити слова "**кібербезпека**" і "**кібердія**" (інакше під визначення підпадатиме і фізичний вплив, що виходить за рамки цього проєкту Закону України про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки, далі – проєкт Закону України) та викласти зазначений пункт в такій редакції:

"кібербезпека мережевих та інформаційних, інформаційно-комунікаційних систем означає здатність електронних комунікаційних мереж та інформаційних, інформаційно-комунікаційних систем витримувати будь-яку **кібер**дію, що може поставити під загрозу (скомпрометувати) доступність, справжність, цілісність або конфіденційність інформації (відомостей, даних), збереженої або переданої чи опрацьованої, або пов'язаних послуг, які пропонують такі електронні комунікаційні мережі та інформаційні, інформаційно-комунікаційні системи, або які доступні за допомогою таких систем";

у пункті 4 і по тексту проєкту Закону України замість терміну "врегулювання інцидентів" вжити сталий термін, що вже використовується в діючій нормативно-правовій базі України, а саме "реагування на кіберінцидент";

у пункті 6 замість слова "**загроза**" вжити слово "**кіберзагроза**" та викласти зазначений пункт в такій редакції:

"кіберзагроза – подія, яка могла б скомпрометувати доступність, справжність, цілісність або конфіденційність збереженої, переданої чи опрацьованої інформації (відомостей, даних) або послуг, що пропонуються електронними комунікаційними мережами та інформаційними системами або доступні через них, але якій вдалося запобігти або яка не відбулася";

у пункті 13 замість словосполучення "**інцидент кібербезпеки (далі – кіберінцидент)** – …" вжити слово "**кіберінцидент - …**", оскільки далі по тексту вживається тільки поняття "кіберінцидент" і не вживається поняття "інцидент кібербезпеки". Це дозволить уникнути надання двох визначень одному й тому ж терміну;

у пункті 18 не визначені критерії оцінки **серйозності** збоїв та **значної** матеріальної чи нематеріальної шкоди, що унеможливлює чітке визначення, які випадки підпадають під зазначене;

у пункті 19 замість слів "**дія**" та "**події**" вжити слова "**кібердія**" та "**кіберподії**" відповідно і викласти зазначений пункт в такій редакції:

"кіберкриза – стан, що виникає внаслідок надзвичайної **кібер**дії та/або **кібер**події, що пов'язана з порушенням або ризиком порушення життєво важливих суспільних функцій (що впливає на невизначену кількість людей та створює

загрози життєво важливим для суспільства та особи інтересів, прав і свобод людини і громадянина;)";

пункт 20 викласти в такій редакції:

"кібероборона – сукупність **політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших** заходів, які спрямовані на досягнення воєнної переваги в кіберпросторі, захист власних мереж суб'єктів сектору безпеки і оборони, нанесення шкоди можливостям, потенціалу, спроможностям та ІКТ противника (його партнерів) у кіберпросторі";

у пункті 21 ("кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших *глобальних* мереж передачі даних") виключити слово "**глобальних**";

у пункті 22 замість поняття "**кіберрозвідка – …**" вжити поняття "**розвідка кіберзагроз – …**", оскільки поняття "кіберрозвідка" означає здобування розвідувальної інформації через кіберпростір;

у пункті 25 ("кібербезпека – діяльність, необхідна для захисту електронних комунікаційних мереж та інформаційних систем, інформаційно-комунікаційних систем, користувачів таких систем та інших осіб, які постраждали від кіберзагроз") доцільно використати визначення **кібербезпеки**, яке прийняте в НАТО, оскільки наведене визначення є спірним (якщо особи не постраждали, то згідно з наведеною редакцією проєкту Закону України виходить, що зазначена діяльність вже не підпадає під визначення "кібербезпека"). Також, це визначення потрібно об'єднати із визначенням, наведеним у пункті 2;

визначення, наведене у пункті 26 ("кіберзагроза – будь-яка потенційна обставина, подія або дія, яка може пошкодити, порушити або інакше негативно вплинути на електронні комунікаційні мережі та інформаційні системи, користувачів таких систем та інших осіб;") доцільно об'єднати з визначенням, наведеним у пункті 6;

доопрацювати пункт 47 ("точка обміну інтернет-трафіком – …"), оскільки він містить незрозуміле формулювання, а саме: "… щоб інтернет-трафік, **що проходить між будь-якою парою беруть участь автономних систем**, …";

пункт 49 ("широкомасштабний інцидент – …") суттєво не відрізняється від визначення, наведеного у пункті 18 ("кіберінцидент зі значним впливом (значний кіберінцидент) – …"). Пропонується виключити визначення, наведені у зазначених пунктах.

Довідково. Категорії (рівні) критичності кіберінцидентів, введені постановою Кабінету Міністрів України від 04 квітня 2023 року № 299 "Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі";

доцільно окремим пунктом додати визначення поняття "**державні інформаційні ресурси**". Зазначений термін вживається, зокрема, в пункті 27 статті 1 та підпункті 3 частини 2 статті 8; проєкту Закону України;

доцільно окремим пунктом додати визначення поняття "**кіберборотьба**". Пропонується таке визначення: "**кіберборотьба** – сукупність взаємоузгоджених за метою, завданнями, місцем та часом заходів визначених військ (сил), спрямованих

на здобуття інформації про кіберінфраструктуру противника, її знищення всіма видами зброї або захоплення (виведення з ладу, отримання контролю), заподіяння їй шкоди шляхом здійснення кібердій та проведення кібероперацій, захист своєї кіберінфраструктури від кіберрозвідки та кібердій противника".

2) у статті 4:

у назві статті 4 вжито термін "**кіберзахист**", а у самій статті він відсутній (у редакції, яка запропонована у проєкті Закону України виключено другу частину цієї статті, що визначала об'єкти кіберзахисту). Тому, пропонується з назви статті 4 ("Об'єкти кібербезпеки та кіберзахисту") виключити слова "**та кіберзахисту**".

у пункті 1 ("Об'єктами кібербезпеки є:") перелічені об'єкти кібербезпеки не відповідають новому визначенню терміну "кібербезпека", зазначеному в статті 1 ("кібербезпека – діяльність, необхідна для захисту електронних комунікаційних мереж та інформаційних систем, інформаційно-комунікаційних систем, користувачів таких систем та інших осіб, які постраждали від кіберзагроз"), тому пропонується доопрацювати наведений перелік об'єктів кібербезпеки;

3) у статті 5^{-1}:

у підпункті 3 пункту 3 ("інформує про кіберзагрози та відповідні методи захисту від них, а також визначає порядок **про** формування переліку кіберзагроз та відповідних методів захисту від них;" виключити зайве слово "**про**";

у підпункті 18 пункту 3 ("забезпечує співробітництво з міжнародними, міжурядовими організаціями, мережами, …") виключити фразу "**є єдиним контактним пунктом, який забезпечує виконання функцій зв'язку для забезпечення транскордонного співробітництва у сфері кібербезпеки**", оскільки наведена редакція унеможливлює співпрацю Міністерства оборони України та Збройних Сил України з НАТО, що несе в собі загрозі національній безпеці України;

4) у статті 5^{-2}:

виключити в повному обсязі статтю 5^{-2} ("Єдиний контактний пункт"), оскільки відбудеться відбір повноважень у Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України, а також обмеження функцій і повноважень інших суб'єктів національної системи кібербезпеки;

5) у статті 5^{-3}:

внести зміни у запропоновану редакцію підпункту 8 пункту 3 ("процедуру взаємного інформування та обміну інформацією між **єдиним контактним пунктом** уповноваженого органу, **єдиним контактним пунктом** Національного координаційного центру кібербезпеки"), оскільки не може одночасно існувати два **єдиних** контактних пункти;

6) у статті 5^{-5}:

доопрацювати пункт 4 зазначеної статті ("Самоідентифікація та ідентифікація суб'єктів виконання вимог з кібербезпеки проводиться кожні чотири роки."), оскільки у ньому наведене незакінчене речення: "Суб'єкт забезпечення вимог з кібербезпеки протягом двох місяців з дня спливу чотирьох років після";

7) у статті 8:

доповнити підпункт 4 пункту 2 новим реченням та викласти його в такій редакції:

"Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО, міжнародними організаціями та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз. **Крім того, Генеральний штаб Збройних Сил України планує військові операції (дії) в кіберпросторі та забезпечує управління ними.** Особливості реалізації Міністерством оборони України, Генеральним штабом Збройних Сил України повноважень у сфері кібербезпеки визначається окремим законом.";

пункт 3 доповнити підпунктом з діючої редакції Закону України:

"**здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору**";

8) у статті 9:

пункт 7 зазначеної статті замість наведеної редакції викласти відповідно до діючої редакції Закону України, оскільки національної команди реагування на кіберінциденти не існує, проте існують інші команди, зокрема MIL.CERT. Тобто, викласти у редакції:

"7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;";

підпункт 1 пункту 2 після слів "на національному" доповнити словами "та галузевому", оскільки в абзаці 1 пункту 2 запропоновано, що "Команди реагування на кіберінциденти, пов'язані з комп'ютерною безпекою (CSIRT), створюються … в секторах з високою критичністю та **інших** критичних секторах, інших споріднених за технологіями оброблення інформації груп/**об'єднань підприємств/установ/організацій** всіх форм власності…". Тобто, викласти зазначений підпункт в такій редакції:

"1) моніторинг та аналіз кіберзагроз, вразливостей та кіберінцидентів на національному **та галузевому** рівні та, за запитом, надання допомоги суб'єктам виконання вимог з кібербезпеки щодо моніторингу в режимі реального часу або майже в реальному часі їхніх електронних комунікаційних мереж та інформаційних систем";

також, пропонується доповнити зазначену статтю пунктом про порядок формування, функціонування та взаємодії відомчих команд реагування на кіберінциденти, пов'язаних з комп'ютерною безпекою (CSIRT);

9) у статті 9[-1]:

абзац 2 пункту 5 після слів "заходів пом'якшення кіберінциденту" доповнити фразою "**крім інформації про кіберінциденти у системах військового призначення**" та викласти в такій редакції:

"Суб'єкт виконання вимог з кібербезпеки у разі відсутності можливості ідентифікувати та повідомити в індивідуальному порядку отримувачів послуг та третіх осіб, які можуть постраждати від кіберінциденту, інформує про кіберінцидент шляхом оприлюднення на своєму веб-сайті або через медіа інформації, необхідної для застосування заходів пом'якшення кіберінциденту **(крім інформації про кіберінциденти у системах військового призначення)"**;

10) щодо статті 17 ("Європейська схема сертифікації кібербезпеки. Рівні довіри до продуктів ІКТ, послуг ІКТ та процесів ІКТ"):

пропонується визначити одну, а не дві схеми сертифікації кібербезпеки. Тобто, або адаптувати національну схему сертифікації кібербезпеки під європейську, або не вводити другу (європейську) схему сертифікації кібербезпеки. Крім того, пропонується здійснити чіткий опис процедури визначення рівнів на основі ризиків щодо ймовірності та можливого впливу кіберінцидентів.

2. Крім того, надаються пропозиції та зауваження до проєкту Закону України у частині, що стосуються охорони державної таємниці та захисту інформації.

Відповідно до Пояснювальної записки прийняття проєкту Закону України обумовлене необхідністю імплементації до українського законодавства положень Директиви (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року (далі – Директива 2022/2555).

Враховуючи, що дія норм Директиви не поширюється на суб'єкти, чия діяльність переважно здійснюється у сферах національної безпеки, громадської безпеки, оборони, або діяльність органів кримінальної юрисдикції, пропонується в тексті проєкту Закону України визначити можливість Міністерству оборони України визначати особливості захисту інформації та забезпечення кібербезпеки електронних комунікаційних мереж та інформаційних систем, інформаційно-комунікаційних систем, власниками яких є сили оборони.

Також проєктом Закону України визначено, що Закон України "Про захист інформації в інформаційно-комунікаційних системах" (Відомості Верховної Ради України, 2005 р., № 26, ст. 347 із наступними змінами) втрачає чинність через два роки з дня, наступного за днем опублікування цього Закону, крім статті 8 Закону, яка діє до дня набрання чинності та введення в дію статті 16 Закону України "Про основні засади забезпечення кібербезпеки України", частини четвертої статті 27-1 Закону України "Про публічні електронні реєстри".

Стаття 16 проєкту Закону України "Про основні засади забезпечення кібербезпеки України" передбачає оцінку відповідності у сфері кібербезпеки продуктів, послуг та процесів інформаційно-комунікаційних технологій та підтвердження відповідності забезпечення заходів кібербезпеки суб'єктами виконання вимог з кібербезпеки при їх використанні та відміняє наявний механізм застосування комплексної системи захисту інформації з підтвердженою відповідністю за результатами державної експертизи у сфері захисту інформації та підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України

щодо систем управління інформаційною безпекою при обробці державних інформаційні ресурси або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Передбачені проєктом Закону України зміни фактично відміняють нормативно-правову базу, що регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та водночас не визначають чітких відмінностей між захистом інформації, технічним захистом інформації та кібербезпекою і не враховують порядок та процедури захисту інформації, в тому числі що становить державну таємницю при її обробці на об'єктах інформаційної діяльності та/або об'єктах електронно-обчислювальної техніки із застосуванням інформаційних (автоматизованих систем), які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем), що може призвести до порушення функціонування системи охорони державної таємниці та захисту інформації з обмеженим доступом в тому числі технічного і криптографічного захисту інформації.

В Статті 27-1. Закону України "Про публічні електронні реєстри" визначено, що власник, держатель національного електронного інформаційного ресурсу, в якому обробляється інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу кібербезпеки або призначає осіб, на яких покладається забезпечення кібербезпеки та контролю за ним.

Водночас зазначаємо, що проєктом Закону України передбачено виключити пункт 2 частини першої статті 2 змін в Закон України "Про основні засади забезпечення кібербезпеки України", що фактично змінює принципи застосування закону та поширює його дію на діяльність пов'язану із кіберзахистом інформації, що становить державну таємницю.

Захист інформації, що становить державну таємницю (криптографічний та технічний) відповідно до закону України "Про державну таємницю" є організаційно-правовою складовою забезпечення охорони державної таємниці, належить до компетенції режимно-секретних органів та підрозділів, які відповідають за забезпечення охорони державної таємниці і виходять за межі повноважень та відповідальності підрозділів кіберзахисту.

Особливості порядку забезпечення кіберзахисту інформації, що становить державну таємницю повинні визначатися державним органом спеціального призначення, який забезпечує державну безпеку відповідно до покладених на нього завдань із забезпечення охорони державної таємниці.

Водночас, відповідно до Стратегії національної безпеки України (затвердженої Указом президента України від 26.05.2015 № 287/2015), одним із пріоритетних напрямів державної політики у сфері національної безпеки України є реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом з урахуванням практики держав-членів НАТО та ЄС. Саме з цією метою, робочою групою Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки із залученням фахівців Служби безпеки України та інших органів державної влади був проведений широкий аналіз міжнародних практик у сфері охорони державної таємниці та опрацьований проєкт Закону України "Про безпеку класифікованої інформації".

Враховуючи зазначене, доцільно першочергово провести реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом з урахуванням практики держав-членів НАТО та ЄС шляхом прийняття Закону України "Про безпеку класифікованої інформації", а вже в подальшому опрацьовувати законопроєкти (вносити зміни, визначати такими, що втрачають чинність існуючі закони), що регулюють діяльність у сфері захисту інформації та кібербезпеки в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

З метою недопущення ризиків порушення функціонування існуючої системи охорони державної таємниці та захисту інформації, та створення потенційних загроз національній безпеці пропонується:

в проєкті Закону України не виключати пункт 2 частини першої статті 2 Закону України "Про основні засади забезпечення кібербезпеки України" до прийняття Закону України "Про безпеку класифікованої інформації";

розглянути можливість надання Міністерству оборони України самостійно визначати особливості захисту інформації у воєнній і оборонних сферах (кіберзахисту) та використання засобів технічного, криптографічного захисту інформації, кіберзахисту, хмарних ресурсів та/або центрів обробки даних в силах оборони відповідно до вже прийнятих постанов Кабінету Міністрів України та Законів України.

Тимчасово виконуючий обов'язки начальника
Головного управління зв'язку та кібербезпеки
Генерального штабу Збройних Сил України –
начальника зв'язку та кібербезпеки
Збройних Сил України
полковник Сергій РАДОМСЬКИЙ