Додаток до листа Телекомпалати України
від 20.07.2021 № 2614

Порівняльна таблиця
до проекту Закону України "Про критичну інфраструктуру" реєстр. № 5219 з пропозиціями та зауваженнями Асоціації «Телекомунікаційна палата України» (ТелПУ)

Редакція законопроекту № 5219	**Редакція законопроекту № 5219 з врахуванням зауважень та пропозиції ТелПУ**	**Обґрунтування/коментарі до зауважень та пропозицій ТелПУ**
Про критичну інфраструктуру	**Про критичну інфраструктуру**	
…	**…**	
Розділ ІІІ **КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ**	**Розділ ІІІ** **КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ**	
…	**…**	
Стаття 9. Сектори критичної інфраструктури	**Стаття 9. Сектори критичної інфраструктури**	
…	..	
4. До життєво важливих функцій порушення яких призводить до негативних наслідків для національної безпеки України відносяться, ~~**зокрема:**~~	4. До життєво важливих функцій порушення яких призводить до негативних наслідків для національної безпеки України відносяться~~:~~	Закон має місити чіткий перелік, без можливості широкого трактування категорії негативних наслідків.
1) урядування та надання найважливіших публічних (адміністративних) послуг;	2) урядування та надання найважливіших публічних (адміністративних) послуг;	
3) енергозабезпечення (в тому числі постачання теплової енергії);	4) енергозабезпечення (в тому числі постачання теплової енергії);	
5) водопостачання та водовідведення;	6) водопостачання та водовідведення;	
7) продовольче забезпечення;	8) продовольче забезпечення;	
9) сільське господарство;	10) сільське господарство;	
11) охорона здоров'я;	12) охорона здоров'я;	
13) фармацевтична промисловість;	14) фармацевтична промисловість;	
15) виготовлення вакцин, стале функціонування біолабораторій;	16) виготовлення вакцин, стале функціонування біолабораторій;	
17) інформаційні та електронні комунікаційні послуги;	9) послуги цифрової інфраструктури, **до якої віднесено:**	Відповідно до NIS 2.0, яку маємо імплементувати в національне законодавство, до цифрової інфраструктури віднесено:

	забезпечення функціонування точок обміну Інтернет-трафіком (IXP); **адміністрування адресного простору українського сегмента Інтернету, у тому числі надання послуг з підтримки та адміністрування систем доменних імен (DNS) в Інтернеті;** **адміністрування та ведення реєстрів доменних імен верхнього рівня в Інтернеті, у тому числі домену.UA;** **надання хмарних послуг, у тому числі зберігання та обробки даних у центрах обробки даних та/або хмарних сховищах, здійснення хмарних обчислень.**	забезпечення функціонування точок обміну Інтернет-трафіком (IXP) адміністрування адресного простору українського сегмента Інтернету, у тому числі надання послуг з підтримки та адміністрування систем доменних імен (DNS) в Інтернеті адміністрування та ведення реєстрів доменних імен верхнього рівня в Інтернеті, у тому числі домену.UA надання хмарних послуг, у тому числі зберігання та обробки даних у центрах обробки даних та/або хмарних сховищах, здійснення хмарних обчислень.
~~18) електронні комунікації, зокрема мобільний зв'язок, радіозв'язок, супутниковий зв'язок та навігація;~~	**виключити**	Дублюється п.9.
…		
Стаття 15. Режими функціонування національної системи захисту критичної інфраструктури		
1. Забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:		
…		
3) режим реагування на виникнення кризової ситуації — суб'єктами національної системи захисту критичної інфраструктури із застосуванням заходів реагування на кризову ситуацію. Функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступу до об'єктів;	3) режим реагування на виникнення кризової ситуації — суб'єктами національної системи захисту критичної інфраструктури із застосуванням заходів реагування на кризову ситуацію. Функціонування інфраструктури відбувається в режимі кризової ситуації, **можуть вводитися** обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступу до об'єктів;	У запропонованій редакції не зрозуміло про які обмеження йде мова, і у чому буде різниця між обмеженнями, передбаченими режимом воєнного стану/надзвичайної ситуації, та мирним часом.
…		
~~3. Рішення щодо оголошення режимів функціонування критичної інфраструктури приймається секторальними органами у сфері захисту~~	**виключити**	В зв'язку з неоднозначним трактуванням та юридичною конструкцією, що дозволяє різночитання – виключити.

~~критичної інфраструктури, відповідальним за сектор критичної інфраструктури.~~		Секторальні органи тільки оголошують певний режим, або ж і передбачають обмеження для приватних компаній? Виходячи з положень вище не зрозуміло про які обмеження йде мова, і у чому буде різниця між обмеженнями, передбаченими режимом воєнного стану/надзвичайної ситуації, та мирним часом.
Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури	**Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури**	
…	**…**	
2. Уповноважений орган у сфері захисту критичної інфраструктури:	2. Уповноважений орган у сфері захисту критичної інфраструктури:	
…	…	
10) готує ~~**висновки та рекомендації**~~ власнику/оператору критичної інфраструктури щодо зміни права власності, цільового призначення чи режиму функціонування об'єкта критичної інфраструктури;	10) готує **пропозиції** власнику/оператору критичної інфраструктури щодо режиму функціонування об'єкта критичної інфраструктури;	Корупційні ризики шляхом встановлення широких дискреційних повноважень органу державної влади за відсутності визначення вичерпних випадків, підстав, форм, строків, порядку здійснення таких повноважень, контролю за їх здійсненням та відповідальності за можливі зловживання під час їх здійснення. Зобов'язання щодо зміни права власності не відповідає вимогам Конституції (ст.41). Не можна рекомендувати особі зміну права власності, оскільки право власності є непорушним в силу ч.4 ст. 41 Конституції України.
…	…	
Стаття 23. Секторальні органи у сфері захисту критичної інфраструктури	**Стаття 23. Секторальні органи у сфері захисту критичної інфраструктури**	
1. Державні органи, які визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури здійснюють наступні завдання:	1. Державні органи, які визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури здійснюють наступні завдання:	
…	…	

1. розробляють та затверджують:	1.розробляють та затверджують:	
~~а) вимоги до захисту об’єктів критичної інфраструктури відповідно до їх категорій;~~	**виключити**	Враховуючи, що відповідно до статті 3 законопроекту, окремим законом регулюються відносини, що виникають при здійсненні заходів, спрямованих на забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури: 1) Не зрозуміло які саме вимоги передбачається, враховуючи, що як ми розуміємо, це стосується фізичного захисту об’єктів: скільки охоронців, які системи сигналізації, або щось інше? 2) Враховуючи відсутність визначення «об’єктів критичної інфраструктури» не зрозуміло стосовно чого такі вимоги будуть застосовуватися: базових станцій, офісів компаній, кабельних ліній?
…	…	
2. затверджують:	3. затверджують:	
…	…	
д) подають операторам об’єктів критичної інфраструктури обов'язкові для розгляду ~~пропозиції~~ з питань захисту критичної інфраструктури ~~та обов’язкові до виконання вимоги щодо усунення причин і умов, які порушують стійкість критичної інфраструктури~~;	д) подають операторам об’єктів критичної інфраструктури **рекомендації** з питань захисту критичної інфраструктури та щодо усунення причин і умов, які порушують стійкість критичної інфраструктури;	Відповідна редакція носить ознаки надмірного та необґрунтованого регуляторного навантаження на приватний бізнес та містить підстави для зловживань, та містить корупційні ризики.
…	…	
Стаття 25. Оператори критичної інфраструктури	**Стаття 25. Оператори критичної інфраструктури**	
1. Основними завданнями операторів критичної інфраструктури є:	1. Основними завданнями операторів критичної інфраструктури є:	
1) забезпечення захисту об’єктів критичної інфраструктури, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, ~~безпеки операційних систем та кібербезпеки;~~	1) забезпечення захисту об’єктів критичної інфраструктури, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки;	Враховуючи, що відповідно до статті 3 законопроекту, окремим законом регулюються відносини, що виникають при здійсненні заходів, спрямованих на забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.
2) розробка та оновлення об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, планів локалізації та ліквідації наслідків аварій, ~~а також заходів кіберзахисту;~~	2) розробка та оновлення об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, планів локалізації та ліквідації наслідків аварій;	Враховуючи, що відповідно до статті 3 законопроекту, окремим законом регулюються відносини, що виникають при здійсненні заходів, спрямованих на забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.

…		
~~**5) оперативне припинення протиправних дій, фізичних атак, спрямованих на відключення або пошкодження роботи операційних систем або систем забезпечення фізичної безпеки об'єкта критичної інфраструктури;**~~	**Виключити**	Суб'єкти підприємницької діяльності обмежені у правових механізмах протидії фізичним атакам. Дане завдання покладено на правоохоронні органи держави.
…	…	
~~**8) участь у заходах з захисту повітряного простору над визначеними об'єктами критичної інфраструктури;**~~	**Виключити**	Не зрозуміло яким чином бізнес може впливати на захист повітряного простору, відповідно норма не однозначна по змісту до застосування.
9) негайне інформування Уповноваженого органу, ~~**органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти,**~~ пов'язані з порушеннями систем фізичної безпеки та кібербезпеки;	9) негайне інформування Уповноваженого органу, **пов'язані з порушеннями систем фізичної безпеки та кібербезпеки відповідно до встановленого Порядку Уповноваженим органом;**	Інформування повинно відбуватися за так званим «принципом єдиного вікна», яким може бути Уповноважений орган. А в свою чергу Уповноважений орган вже в порядку взаємодії може повідомляти інші державні органи. Враховуючи, що відповідно до статті 3 законопроекту, окремим законом регулюються відносини, що виникають при здійсненні заходів, спрямованих на забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.
~~**10) забезпечення постійного зв'язку з відповідальними за реагування та з іншими компетентними організаціями та установами;**~~	**Виключити**	Не відповідає принципу юридичної визначеності. Компанії можуть забезпечити зв'язок тільки з власними співробітниками і не можуть відповідати за зв'язок з іншими установами.
…	…	
~~**12) створення і використання необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків;**~~	**Виключити**	Призводить до незапланованих суттєвих додаткових витрат та містить ознаки втручання в господарську діяльність підприємства
…	…	
~~**14) захист інформації про системи управління, зв'язку, фізичну та кібербезпеку, забезпечення**~~	14) захист інформації про системи управління, зв'язку, фізичну, забезпечення відповідно до встановлених	Враховуючи, що відповідно до статті 3 законопроекту, окремим законом регулюються відносини, що

~~**відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об'єкти критичної інфраструктури;**~~	законодавством вимог конфіденційності інформації під час оброблення даних про об'єкти критичної інфраструктури;	виникають при здійсненні заходів, спрямованих на забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.
…	…	
4. Оператори критичної інфраструктури зобов'язані:	4. Оператори критичної інфраструктури зобов'язані:	
…	…	
~~**3) завчасно, але не менше ніж за тридцять календарних днів до дати зміни стану об'єкта критичної інфраструктури або його частини, інформувати Уповноважений орган у сфері захисту критичної інфраструктури про наміри змінити цільове призначення, режим функціонування чи намір передати права на об'єкт критичної інфраструктури та виконувати надані йому висновки та рекомендації;**~~	3**) протягом тридцяти календарних днів з дати настання змін, інформувати уповноважений орган про зміну цільового призначення чи режиму функціонування об'єкта критичної інфраструктури;**	Оператор не може завчасно інформувати про події, які не були ним заплановані.
~~**4) щорічно надавати інформацію про виконання повноважень відповідно до цього Закону, за формою, визначеною Кабінетом Міністрів України;**~~	**Виключити**	Не відповідає принципу адекватності та доцільності регулювання. Питання мети збору звітів є відкритим. Законопроектом передбачено паспортизацію ОКІ. Впроваджується додаткове звітне навантаження для подання таких щорічних форм. Крім того не визначено, якими повноваженнями наділено операторів КІ.
…	…	
Розділ V	**Розділ V**	
ОРГАНІЗАЦІЙНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	**ОРГАНІЗАЦІЙНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**	
Стаття 26. Планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури	**Стаття 26. Планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури**	
…	…	
6. На об'єктовому рівні:	6. На об'єктовому рівні:	
оператори критичної інфраструктури на кожному об'єкті критичної інфраструктури розробляють та	оператори критичної інфраструктури на кожному об'єкті критичної інфраструктури розробляють та	Враховуючи, що відповідно до статті 3 законопроекту, окремим законом регулюються відносини, що

забезпечують виконання об'єктового плану заходів щодо захисту і забезпечення стійкості критичної інфраструктури, який включає заходи з фізичного захисту, протидії загрозам, забезпечення безпеки інформації ~~та кібербезпеки~~ на об'єктах критичної інфраструктури.	забезпечують виконання об'єктового плану заходів щодо захисту і забезпечення стійкості критичної інфраструктури, який включає заходи з фізичного захисту, протидії загрозам, забезпечення безпеки інформації на об'єктах критичної інфраструктури.	виникають при здійсненні заходів, спрямованих на забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.
Стаття 29. Державно-приватне партнерство у сфері захисту критичної інфраструктури	**Стаття 29. Державно-приватне партнерство у сфері захисту критичної інфраструктури**	
1. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється шляхом:	1. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється шляхом:	
…	…	
~~**1) забезпечення резервування основних ресурсів для функціонування критичної інфраструктури у різних режимах;**~~	Виключити	Призводить до незапланованих суттєвих додаткових витрат та містить ознаки втручання в господарську діяльність підприємства Нечіткість, з порушенням принципу юридичної визначеності, регламентації обов'язку «резервування основних ресурсів», при відсутності конкретно встановленого показника такого «резервування».
~~**2) організації системи оповіщення населення та суб'єктів господарювання про інциденти та кризові ситуації на об'єктах критичної інфраструктури;**~~	Виключити	Організація оповіщення населення врегульована Кодексом цивільного захисту України. Призводить до незапланованих суттєвих додаткових витрат та містить ознаки втручання в господарську діяльність підприємства
~~3) створення системи самооцінки віднесення об'єктів критичної інфраструктури за критеріями, визначеними цим Законом, створення інформаційних ресурсів для підвищення рівня знань із захисту об'єктів критичної інфраструктури;~~	Виключити	В чому тут партнерство? Яким нормам закону про Державно-приватне партнерство відповідають ці пункти?
~~**4) створення механізмів для саморегулювання, обміну інформацією між операторами об'єктів критичної інфраструктури у певному секторі;**~~	Виключити	В чому тут партнерство? Яким нормам закону про Державно-приватне партнерство відповідають ці пункти?
~~**5) створення та підтримки розвитку систем сертифікації та оцінки відповідності у секторах критичної інфраструктури;**~~	Виключити	Або перенести в обов'язки державних органів. **Потребує додаткового обговорення**. Сертифікація чого саме?
~~**6) створення сприятливих умов для запровадження системи добровільного**~~	Виключити	В чому тут партнерство?

~~**страхування від потенційних ризиків і загроз для об'єктів критичної інфраструктури.**~~		Яким нормам закону про Державно-приватне партнерство відповідають ці пункти? Для порівняння із ст. 36 Ч. 1.
…		
Стаття 33. Відповідальність за порушення законодавства у сфері захисту критичної інфраструктури		
…		
~~**2. У разі у порушення законодавства у сфері захисту критичної інфраструктури, до суб'єктів перерахованих у частині першій цієї статті, можуть бути застосовані такі адміністративно-господарські санкції:**~~	Виключити	1. Незрозуміло про що йдеться. 2. Незрозуміло яким чином порушення законодавства у сфері захисту критичної інфраструктури кореспондуються з порушеннями здійснення господарської діяльності, саме за які і встановлено адміністративно-господарські санкції (Господарський кодекс України). 3. Не визначено орган державної влади, який буде накладати санкції. 4. Яким чином будуть накладатися такі санкції на органи державної влади? Законопроектом не визначено порядок та підстави застосування перерахованих адміністративно-господарських санкцій, а також повноваження будь-яких суб'єктів приймати рішення щодо накладення таких санкцій. Крім того даним законом взагалі не регулюються господарські відносини, відповідно до преамбули цей Закон визначає правові та організаційні засади функціонування та захисту критичної інфраструктури і є складовою законодавства України у сфері національної безпеки.
~~**адміністративно-господарський штраф;**~~	Виключити	Проектом не передбачено склад правопорушення, за яке може накладатися штраф та його розмір.
~~**стягнення зборів (обов'язкових платежів);**~~	Виключити	Не зрозуміло, які збори передбачено стягувати додатково.

~~**обмеження або зупинення діяльності суб'єкта господарювання.**~~	Виключити	Припиняти діяльність підприємства це надмірна санкція, її наявність може призвести до зловживань та погіршення інвестиційного клімату в Україні. У контексті саме критичної, тобто життєвоважливої інфраструктури, заборона діяльності виглядає нелогічною.
~~**3. У разі порушення законодавства у сфері захисту критичної інфраструктури, що містить ознаки адміністративного правопорушення та/ або суспільно небезпечного діяння, яке містить склад кримінального правопорушення, такі особи мають бути притягнуті до відповідальності відповідно до законодавства України про кримінальну відповідальність, та/або до законодавства України про адміністративні правопорушення.**~~	Виключити	Виключити, або передбачити зміни до Кодексів окремим проектом який повинен бути поданий пакетом.
Стаття 36. Страхування ризиків		
~~**1. Власники та/або керівники підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури забезпечують страхування ризику фінансових втрати, викликаних кризовою ситуацією відповідно до Закону України «Про страхування».**~~	1. Власники та/або керівники підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури **на добровільних засадах можуть страхувати** ризики **пошкодження або знищення майна об'єктів критичної інфраструктури або їх елементів**, викликаних кризовою ситуацією відповідно до Закону України «Про страхування».	Ст. 29. Частина 1 п. 15 встановлює добровільну участь у страхуванні. Чи страхувати втрату прибутку, чи будь-яких інших фінансових ризиків має вирішувати суб'єкт господарювання, зокрема і оператор критичної інфраструктури, самостійно. Страхування фінансових ризиків чинним законом передбачено як добровільне (п. п. 18 ч. 4, ст.6 Закона про страхування)
~~**2. Перелік об'єктів критичної інфраструктури, страхових ризиків, щодо яких здійснюється обов'язкове державне страхування ризику фінансових втрати, викликаних кризовою ситуацією, затверджується Кабінетом Міністрів України.**~~	2. Об'єкти критичної інфраструктури, **які відносяться до І категорії критичності,** підлягають обов'язковому державному страхуванню. Перелік страхових ризиків щодо таких об'єктів затверджується Кабінетом Міністрів України.	Обов'язково повинні страхуватись Об'єкти критичної інфраструктури, **які відносяться до І категорії критичності**
Розділ VI		
ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ		

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування та вводиться в дію через шість місяців з дня набрання ним чинності.		
Через 3 роки з дня набрання чинності цим Законом набувають чинності положення:		
про обов'язкове страхування об’єктів критичної інфраструктури, - частина друга статті 36 та абзац другий підпункту 20 пункту 2 цього Закон,	про обов'язкове страхування об’єктів критичної інфраструктури, - частина друга статті 36 та абзац другий підпункту 20 пункту 2 **Розділу VI** цього Закону,	Редакційно уточнити зміст положення
~~**про запровадження адміністративно-господарської відповідальності у разі у порушення законодавства у сфері захисту критичної інфраструктури, - частина друга статті 33 цього Закону.**~~	**Виключити.**	Адміністративно-господарські санкції застосовуються до суб'єктів господарювання за порушення ними правил здійснення господарської діяльності! Даний законопроект не регулює господарську діяльність. (Господарський кодекс України)
До приведення у відповідність із цим Законом законодавчі та інші нормативно-правові акти застосовуються в частині, що не суперечить цьому Закону.		
2. Внести до законів України такі зміни:		
…		
~~**5) частину другу статті 6 Закону України “Про охоронну діяльність”** (Відомості Верховної Ради України, 2013 р., № 2, ст. 8) викласти в такій редакції:~~	**виключити**	Дані зміни можуть призвести до обмеження можливості операторів залучати приватні компанії для охорони об’єктів та відповідно монополізації та зростання вартості таких послуг.
~~“Перелік об’єктів критичної інфраструктури, охорона яких здійснюється державними органами, підприємствами та організаціями, затверджується Кабінетом Міністрів України.”;~~		
…	…	
11) у Законі України “Про основні засади забезпечення кібербезпеки України” (Відомості Верховної Ради України, 2017 р., № 45, ст.403):	**11) у Законі України “Про основні засади забезпечення кібербезпеки України”** (Відомості Верховної Ради України, 2017 р., № 45, ст.403):	
у статті 1:	у статті 1:	

пункт 16 виключити;	пункт 16 виключити;	
~~**частину другу доповнити реченням такого змісту :**~~		
~~**“Термін “об’єкт критичної інфраструктури” вживаються в цьому Законі у значенні, визначеному Законом України “Про критичну інфраструктуру”;**~~	**виключити**	У даному законопроєкті таке визначення відсутнє.
…		
20) У Законі України "Про страхування" (Відомості Верховної Ради України, 2002 р., № 7, ст. 50 із наступними змінами) :		
частину четверту статті 6 після пункту 22 доповнити новим пунктом такого змісту:		
“22-1) страхування ~~**ризику фінансових втрат, викликаних кризовою ситуацією на**~~ об’єкті критичної інфраструктури; ”;	“22-1) страхування **об’єктів критичної інфраструктури** або їх елементів; ”;	Редакційне уточнення об’єкта страхування
частину першу статті 7 після пункту 49 доповнити новим пунктом 50 такого змісту:		
«50) страхування ~~**ризику фінансових втрат, викликаних кризовою ситуацією на**~~ об’єкті критичної інфраструктури віднесеному до Переліку, що затверджується Кабінетом Міністрів України відповідно до Закону України “Про критичну інфраструктуру”;	«50) **страхування об’єктів критичної інфраструктури та їх елементів, які відносяться до І категорії критичності, визначених** відповідно до Закону України “Про критичну інфраструктуру”;	Редакційне уточнення об’єкта страхування
…		