Додаток до вих. ІнАУ № 04/1-4 від 25.01.2023

ПОРІВНЯЛЬНА ТАБЛИЦЯ

до проекту Закону України «Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури»

Зміст положення (норми) чинного акта законодавства	Зміст відповідного положення (норми) проєкту акта	Пропозиції ІнАУ
Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»		
Стаття 14. Обов'язки Державної служби спеціального зв'язку та захисту інформації України Відсутнє	**Стаття 14. Обов'язки Державної служби спеціального зв'язку та захисту інформації України** … 97) встановлення порядку підтвердження відповідності впроваджених заходів безпеки інформації встановленим вимогам постачальниками та їх субпідрядниками, які постачають товари, роботи, послуги, що забезпечують функціонування інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури замовникам, визначеним у частині першій статті 2 Закону України "Про публічні закупівлі", та операторам критичної інфраструктури; **…** 104) погодження в порядку, встановленому законодавством, призначення офіцерів із кіберзахисту, на яких покладається забезпечення захисту інформації та кіберзахисту в державних органах, установах, організаціях, органах місцевого самоврядування ~~та на об'єктах критичної інфраструктури~~;	**Виключити** *Коментар: така редакція може мати наслідком те, що такі вимоги будуть встановлюватись абсолютно до усіх постачальників та субпідрядників. Відтак, потрібно конкретизувати, які саме товари, роботи, послуги або зазначити, що їх перелік буде встановлюватись окремим нормативно-правовим актом.* *Доцільніше встановлювати вимоги не до постачальників та субпідрядників, а вимоги для товарів, робіт, послуг.* **…** 104) погодження в порядку, встановленому законодавством, призначення офіцерів із кіберзахисту, на яких покладається забезпечення захисту інформації та кіберзахисту в державних органах, установах, організаціях, органах місцевого самоврядування;

		Коментар: По-перше, об'єкти критичної інфраструктури, в своїй переважній більшості, це суб'єкти приватної власності і кожен власник, керівник може призначати на посади фахівців, які, в першу чергу, відповідають запитам та вимогам суб'єкта господарювання. Будь-яких вимог чи встановлення права державних органів втручатись в діяльність субєктів господарювання шляхом призначення певних осіб на певні посади законодавством не передбачено, в т.ч. таке не встановлено і в КЗпП України. По-друге, на сьогодні, перелік об'єктів критичної інфраструктури не складено у порядку, встановленому Законом України «Про критичну інфраструктуру». Проте, з огляду на положення законодавства, кількість субєктів господарювання, які є об'єктами критичної інфраструктури, може бути достатньо значною. Відтак, працівники ДССЗЗІ не матимуть технічної можливості розглянути кандидатури та погодити офіцерів із кіберзахисту на усіх об'єктах, запропонованих у зазначеному положенні проекту Закону. **Із зазначених мотивів, у статті 5-1, якою пропонується доповнити Закон України «Про основні засади забезпечення кібербезпеки України» також виключити аналогічне положення щодо погодження ДССЗЗІ офіцерів із кіберзахисту на об'єктах критичної інфраструктури.*
Стаття відсутня	**Стаття 26. Основні засади здійснення державного контролю** … 2. Контроль за технічним захистом інформації та кіберзахистом здійснюється щодо виконання власниками, розпорядниками інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси та/або інформація,	2. Контроль за технічним захистом інформації та кіберзахистом здійснюється щодо виконання власниками, розпорядниками інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси та/або інформація,

	вимога щодо захисту якої встановлена законом, а також щодо операторів критичної інфраструктури відносно захисту критичної технологічної інформації та кіберзахисту критичної інформаційної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України), а також щодо постачальників та їх субпідрядників, які поставляють товари, роботи, послуги, що забезпечують функціонування інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури замовникам, визначеним у частині першій статті 2 Закону України "Про публічні закупівлі", та операторам критичної інфраструктури (далі – об'єкти контролю). …	вимога щодо захисту якої встановлена законом, а також щодо операторів критичної інфраструктури **I та II категорії критичності** відносно захисту критичної технологічної інформації та кіберзахисту критичної інформаційної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України), а також щодо постачальників та їх субпідрядників, які поставляють товари, роботи, послуги, що забезпечують функціонування інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури замовникам, визначеним у частині першій статті 2 Закону України "Про публічні закупівлі", та операторам критичної інфраструктури **I та II категорії критичності** (далі – об'єкти контролю). *Коментар тут і далі: розповсюдження державного контролю і регулювання на операторів критичної інфраструктури III та IV категорії (з незначними наслідками негативного впливу), які зазвичай є малими і мікропідприємствами, недоцільно через те, що такі підприємства не мають ресурсів для відповідних заходів, а також через те, що це перевантажить відповідну державну систему контролю і регулювання.*
	10. Посадові особи Державної служби спеціального зв'язку та захисту інформації України, уповноважені на здійснення заходів контролю за технічним захистом інформації та кіберзахистом, при здійсненні таких заходів мають право: …	
	2) доступу (з урахуванням вимог нормативно-правових актів щодо охорони державної таємниці в	2) доступу **у робочий час** (з урахуванням вимог нормативно-правових актів щодо охорони

	Україні) до території, будівлі, споруди, приміщення, інших об'єктів об'єкта контролю для вивчення питань, безпосередньо пов’язаних з проведенням державного контролю за технічним захистом інформації та кіберзахистом; … 7) отримувати та безпосередньо фіксувати інформацію, в тому числі з обмеженим доступом з дотриманням відповідних зобов'язань щодо її охорони, про порушення умов експлуатації інформаційних, інформаційно- комунікаційних систем та об'єктів критичної інформаційної інфраструктури шляхом створення скріншотів та використання засобів фото-, відеозйомки з урахуванням вимог щодо охорони державної таємниці;	державної таємниці в Україні) до території, будівлі, споруди, приміщення, інших об'єктів об'єкта контролю для вивчення питань, безпосередньо пов’язаних з проведенням державного контролю за технічним захистом інформації та кіберзахистом; … 7) отримувати та безпосередньо фіксувати інформацію, в тому числі з обмеженим доступом з дотриманням відповідних зобов'язань щодо її охорони, про порушення умов експлуатації інформаційних, інформаційно- комунікаційних систем **в яких обробляються державні інформаційні ресурси та/або інформація, вимога щодо захисту якої встановлена законом**, та об'єктів критичної інформаційної інфраструктури **I та II категорії критичності** шляхом створення скріншотів та використання засобів фото-, відеозйомки з урахуванням вимог щодо охорони державної таємниці;
Закон України «Про основні засади забезпечення кібербезпеки України»		
Стаття 5. Суб'єкти забезпечення кібербезпеки Відсутнє	**Стаття 5. Суб'єкти забезпечення кібербезпеки** **…** 7) оператори критичної інфраструктури	7) оператори критичної інфраструктури **I та II категорії критичності**
Стаття відсутня	**Стаття 5[1]. Підрозділи із кіберзахисту, офіцери із кіберзахисту** 1. В органах державної влади, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворюються підрозділи із кіберзахисту та призначаються офіцери із кіберзахисту, яким	

	безпосередньо підпорядковуються підрозділи із кіберзахисту. Оператори критичної інфраструктури призначають відповідальну особу, яка виконує завдання офіцера із кіберзахисту, та за необхідності з метою належного виконання основних вимог з кіберзахисту створюють підрозділ із кіберзахисту. Призначення офіцера із кіберзахисту на посаду в органах державної влади, ~~на об'єктах критичної інфраструктури I та II категорії критичності~~ та його посадові інструкції погоджуються Адміністрацією Держспецзв'язку, після перевірки в межах своїх повноважень Службою безпеки України.	Оператори критичної інфраструктури **I та II категорії критичності** призначають відповідальну особу, яка виконує завдання офіцера із кіберзахисту, та за необхідності з метою належного виконання основних вимог з кіберзахисту створюють підрозділ із кіберзахисту. Призначення офіцера із кіберзахисту на посаду в органах державної влади та його посадові інструкції погоджуються Адміністрацією Держспецзв'язку, після перевірки в межах своїх повноважень Службою безпеки України. *Коментар: див. аргументацію до п.104 ст.14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»*
Стаття 6. Об'єкти критичної інфраструктури Відсутнє	**Стаття 6. Об'єкти критичної інфраструктури** 1. Власники та посадові особи операторів критичної інфраструктури зобов'язані виконувати основні вимоги щодо кіберзахисту об'єктів критичної інфраструктури, надання обов'язкових повідомлень про інциденти кібербезпеки, кіберзагрози, кібератаки та виконувати інші зобов'язання щодо захисту інформації та кіберзахисту відповідно до законодавства та несуть відповідальність за їх невиконання відповідно до закону. … 3. Вимоги до заходів безпеки інформації, які повинні бути впроваджені постачальниками, включаючи їх субпідрядників, товарів, робіт та послуг, що забезпечують функціонування інформаційних, електронних комунікаційних та	**Стаття 6. Об'єкти критичної інфраструктури** 1. Власники та посадові особи операторів критичної інфраструктури **I та II категорії критичності** зобов'язані виконувати основні вимоги щодо кіберзахисту об'єктів критичної інфраструктури, надання обов'язкових повідомлень про інциденти кібербезпеки, кіберзагрози, кібератаки та виконувати інші зобов'язання щодо захисту інформації та кіберзахисту відповідно до законодавства та несуть відповідальність за їх невиконання відповідно до закону. … 3. Вимоги до заходів безпеки інформації, які повинні бути впроваджені постачальниками, включаючи їх субпідрядників, товарів, робіт та послуг, що забезпечують функціонування інформаційних, електронних комунікаційних та

	інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури замовникам, визначеним у частині першій статті 2 Закону України "Про публічні закупівлі", та операторам критичної інфраструктури, порядок визначення рівня ризику, пов’язаного з постачанням таких товарів, робіт та послуг, та порядок підтвердження постачальниками відповідності щодо впроваджених заходів безпеки інформації, встановлюються Державною службою спеціального зв’язку та захисту інформації України.	інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури замовникам, визначеним у частині першій статті 2 Закону України "Про публічні закупівлі", та операторам критичної інфраструктури **I та II категорії критичності**, порядок визначення рівня ризику, пов’язаного з постачанням таких товарів, робіт та послуг, та порядок підтвердження постачальниками відповідності щодо впроваджених заходів безпеки інформації, встановлюються Державною службою спеціального зв’язку та захисту інформації України.
Стаття відсутня	**Стаття 9[1]. Обмін інформацією про інциденти кібербезпеки та кібератаки** … 3. Власники та розпорядники інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури, зобов'язані повідомляти про всі інциденти кібербезпеки, кібератаки. ~~Оператори критичної інфраструктури зобов'язані повідомляти про всі значні інциденти кібербезпеки, кібератаки, відносно об'єктів критичної інформаційної інфраструктури~~. … 6. Посадові особи власників, розпорядників інформаційних, електронних комунікаційних та	 3. Власники та розпорядники інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури **I та II категорії критичності** зобов'язані повідомляти про всі інциденти кібербезпеки, кібератаки. **Виключити** *Коментар: дублювання вимоги в попередньому абзаці* … 6. Посадові особи власників, розпорядників інформаційних, електронних комунікаційних та

	інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, операторів критичної інфраструктури, несуть адміністративну відповідальність відповідно до закону за невиконання або невиконання у встановлені строки обов'язку надання обов'язкових повідомлень про інциденти кібербезпеки, кібератаки. ~~7. Інформація про інцидент кібербезпеки, кібератаку щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури, є інформацією з обмеженим доступом, крім випадків, коли порядком обміну такою інформацією або на підставі інших вимог законодавства передбачається обов'язок щодо її розкриття з визначеною метою.~~	інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, операторів критичної інфраструктури **I та II категорії критичності**, несуть адміністративну відповідальність відповідно до закону за невиконання або невиконання у встановлені строки обов'язку надання обов'язкових повідомлень про інциденти кібербезпеки, кібератаки. **Виключити** *Коментар: в разі впроваждення такої новації всі оператори критичної інфраструктури мають створювати підрозділ з технічного захисту інформації або призначати осіб, на яких покладається забезпечення захисту інформації від витоку технічними каналами та контролю за ним*
Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України Відсутнє	**Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України** … 4. Державна служба спеціального зв'язку та захисту інформації України здійснює державний контроль за додержанням вимог законодавства у сфері кіберзахисту власниками, розпорядниками інформаційно- комунікаційних систем, в яких обробляються державні інформаційні ресурси та/або інформація, вимога щодо захисту якої встановлена законом, а також операторами критичної інфраструктури в частині використання ними комунікаційних та технологічних систем	… 4. Державна служба спеціального зв'язку та захисту інформації України здійснює державний контроль за додержанням вимог законодавства у сфері кіберзахисту власниками, розпорядниками інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси та/або інформація, вимога щодо захисту якої встановлена законом, а також операторами критичної інфраструктури **I та II категорії критичності** в частині використання ними комунікаційних та технологічних систем (крім

	(крім об'єктів критичної інфраструктури у банківській системі України).	об'єктів критичної інфраструктури у банківській системі України).
Закон України «Про захист інформації в інформаційно-комунікаційних системах»		
Стаття 1. Визначення термінів Відсутнє	**Стаття 1. Визначення термінів** об’єкт інформаційної діяльності – інженерно-технічна споруда (будівля, приміщення тощо), відокремлена територія (зона), транспортний засіб, намет, де провадиться діяльність, пов’язана з державними інформаційними ресурсами та інформацією, вимога щодо захисту якої встановлена законом; … обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів, або автономно (без підключення до інших засобів обробки інформації, ліній зв’язку або мереж передачі даних) пристроями обробки інформації;	*Коментар:* *Застосування у законі пропонованих визначень об’єкта інформаційної діяльності і обробки інформації в системі вважаємо таким, що не відповідає принципу визначеності.* *Визначення об’єкта інформаційної діяльності і обробки інформації в системі потребує доопрацювання і більшої контретизації. В пропонованій редакції під ці визначення потрапляє необмежений круг суб’єктів господарювання в сфері інформації, які можуть необгрунтовано потрапити під заходи державного регулювання.*
Стаття 10. Повноваження державних органів у сфері захисту інформації в системах Відсутнє	**Стаття 10. Повноваження державних органів у сфері захисту інформації в системах та на об’єктах інформаційної діяльності** **…** здійснює державний контроль за додержанням вимог законодавства у сфері технічного захисту інформації та кіберзахисту власниками, розпорядниками інформаційно- комунікаційних систем, в яких обробляються державні інформаційні ресурси та/або інформація, вимога щодо захисту якої встановлена законом, а також операторами критичної інфраструктури в частині використання ними комунікаційних та технологічних систем (крім об'єктів критичної інфраструктури у банківській системі України);	здійснює державний контроль за додержанням вимог законодавства у сфері технічного захисту інформації та кіберзахисту власниками, розпорядниками інформаційно- комунікаційних систем, в яких обробляються державні інформаційні ресурси та/або інформація, вимога щодо захисту якої встановлена законом, а також операторами критичної інфраструктури **І та ІІ категорії критичності** в частині використання ними комунікаційних та технологічних систем (крім

		об'єктів критичної інфраструктури у банківській системі України);
	По тексту проекту Закону застосовуються такі вирази, як «відповідні професійні стандарти» (п. 113 ст. 14 ЗУ «Про Державну службу спеціального зв'язку та захисту інформації України»), «відповідні співробітники основних суб'єктів забезпечення кібербезпеки України» (ч.8 ст.26 ЗУ «Про Державну службу спеціального зв'язку та захисту інформації України»), «відповідні завдання від національного CSIRT» (п.13 ч.3 ст. 9 ЗУ «Про основні засади забезпечення кібербезпеки України»).	Застосування у законі наведених виразів вважаємо таким, що не відповідає принципу визначеності, оскільки у наведених випадках не встановлено чітко вимоги, тому, кожен, при застосуванні цього закону може трактувати слово «відповідні» на свою користь. Закон із застосуванням таких нечітких положень не буде реалізованим. Відтак, зазначені положення потребують доопрацювання з метою їх чіткості.