Додаток до листа Телекомпалати
від 21.05.2021 № 2597

ПОРІВНЯЛЬНА ТАБЛИЦЯ
до Закону України «Про внесення змін до Закону України "Про Службу безпеки України" щодо удосконалення організаційно-правових засад діяльності Служби безпеки України

Текст законопроекту	Пропозиції Асоціації «Телекомунікаційна палата України»	Коментар
І. Внести до Закону України «Про Службу безпеки України» (Відомості Верховної Ради України, 1992 р., № 27, ст. 382 із наступними змінами) зміни, виклавши його в такій редакції:		
Стаття 13. Збирання та отримання інформації Службою безпеки України 1. Для забезпечення виконання покладених на Службу безпеки України завдань її силами та засобами відповідно до законодавства здійснюється збирання та отримання інформації, у тому числі персональних даних, шляхом: здійснення моніторингу джерел інформації, а також інших заходів, спрямованих на збирання інформації;		
отримання у встановленому порядку на безоплатній основі інформації від правоохоронних та інших державних органів, військових формувань, органів місцевого самоврядування, ~~**підприємств, установ, організацій;**~~	**Виключити слова «підприємств, установ, організацій»**	Для зменшення корупційних проявів та ризиків обмеження прав громадського сектору, бізнесу, права людини. Законопроект (ст. 25) передбачає взаємодію СБУ з підприємствами установами, організаціями, а новий абзац, що пропонується доповнити до цієї частини статті 13 - конкретизує умови отримання інформації та її розпорядників.
здійснення обміну інформацією, у тому числі розвідувальною, з розвідувальними		

органами у порядку, визначеному спільними актами;		
відсутній	**Доповнити новим абзацом:** **Служба безпеки України має право у встановленому законом порядку та виключно на підставі рішення суду отримувати інформацію, яка містить комерційну та банківську таємницю, персональні дані фізичних осіб від підприємств, установ, організацій та фізичних осіб**	Статтею 64 Конституції України гарантовано, що конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України. Тому подання суб'єктами господарювання та фізичними особами інформації працівникам СБУ має відбуватись з обов'язковим дотриманням вимог ст. ст. 31, 32 Конституції України, зокрема, виключно на підставі судового рішення у випадках, передбачених цими статтями. Інформація, що передбачається до витребування СБУ містить персональні дані, а тому повинна надаватися виключно на підставі рішення суду.
2. Отримання Службою безпеки України інформації може здійснюватися на підставі запиту, підписаного начальником (керівником) або заступником начальника (керівника) функціонального підрозділу Центрального управління Служби безпеки України або регіонального органу Служби безпеки України. Суб'єкти, яким адресовано зазначений запит, зобов'язані протягом п'яти робочих днів надати Службі безпеки України запитувану інформацію. У разі неможливості надання запитуваної інформації такий суб'єкт	**Виключити слова «**але не більше ніж на п'ять робочих днів.»	З досвіду отримання запитів державних органів, максимальні 5 робочих днів для надання відповіді на запит може виявитися недостатнім. Пропонуємо прибрати обмеження щодо максимального строку продовження відповіді на запит.

повинен невідкладно у письмовій формі повідомити про це підрозділ Служби безпеки України, який звернувся із запитом, з обґрунтуванням причин неможливості надання інформації. Служба безпеки України за зверненням відповідного суб'єкта може продовжити строк надання інформації, ~~**але не більше ніж на п'ять робочих днів.**~~		
…		
4. З метою попередження та припинення посягань на державний суверенітет, конституційний лад і територіальну цілісність України, злочинів проти миру та безпеки людства, протидії тероризму та розвідувально-підривної діяльності, Служба безпеки України також може отримувати: 1) інформацію, яка знаходиться в операторів та провайдерів телекомунікацій про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; 2) інформацію від банків, депозитарних, фінансових та інших установ, підприємств та організацій незалежно від форми власності про операції, рахунки, вклади, правочини фізичних та юридичних осіб. Отримання інформації, яка містить банківську таємницю або міститься у системі депозитарного обліку цінних	4. З метою попередження та припинення посягань на державний суверенітет, конституційний лад і територіальну цілісність України, злочинів проти миру та безпеки людства, протидії тероризму та розвідувально-підривної діяльності, Служба безпеки України також може отримувати: 1) **на підставі рішення суду** інформацію, яка знаходиться в операторів та провайдерів телекомунікацій про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; 2) інформацію від банків, депозитарних, фінансових та інших установ, підприємств та організацій незалежно від форми власності про операції, рахунки, вклади, правочини фізичних та юридичних осіб. Отримання інформації, яка містить банківську таємницю або міститься у	Статтею 64 Конституції України гарантовано, що конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України. Тому подання суб'єктами господарювання та фізичними особами інформації працівникам СБУ має відбуватись з обов'язковим дотриманням вимог ст. ст. 31, 32 Конституції України, зокрема, виключно на підставі судового рішення у випадках, передбачених цими статтями. Інформація, що передбачається до витребування СБУ містить персональні дані, а тому повинна надаватися виключно на підставі рішення суду.

паперів, здійснюється в порядку та обсязі, визначених Законом України "Про банки і банківську діяльність", Законом України "Про депозитарну систему України" з урахуванням положень частини другої цієї статті.	системі депозитарного обліку цінних паперів, здійснюється в порядку та обсязі, визначених Законом України "Про банки і банківську діяльність", Законом України "Про депозитарну систему України" з урахуванням положень частини другої цієї статті.	
…	…	
II. Прикінцеві та перехідні положення 1. Цей Закон набирає чинності з дня, наступного за днем його опублікування, крім частини п'ятої статті 8 яка набирають чинності з 1 січня 2024 року.		
…		
14. Внести зміни до таких законодавчих актів України: …		
12) у Законі України "Про контррозвідувальну діяльність" (Відомості Верховної Ради України, 2003 р., № 12, ст. 89 із наступними змінами):		
..		
е) у статті 7: пункт 3 замінити пунктами такого змісту:	е) у статті 7: пункт 3 замінити пунктами такого змісту:	
…	…	
3-5) здійснювати тимчасове обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою	3-5) **на підставі рішення суду** здійснювати тимчасове обмеження доступу до визначених (ідентифікованих)	Такі заходи можуть бути вжиті в ході контррозвідувальної діяльності органами, підрозділами та співробітниками Служби

недопущення терористичного акту або протидії розвідувально-підривної діяльності на шкоду Україні, протидії проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації, тих які використовуються для організації, підготовки, вчинення, фінансування, сприяння або приховування акту несанкціонованого втручання в діяльність об'єктів критичної інформаційної інфраструктури, з використанням технічних засобів, ~~що встановлюються операторами, провайдерами телекомунікацій та іншими суб'єктами господарювання~~;	інформаційних ресурсів (сервісів) з метою недопущення терористичного акту або протидії розвідувально-підривної діяльності на шкоду Україні, протидії проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації, тих які використовуються для організації, підготовки, вчинення, фінансування, сприяння або приховування акту несанкціонованого втручання в діяльність об'єктів критичної інформаційної інфраструктури, з використанням технічних засобів;	безпеки України за рішенням суду з використанням вже існуючих засобів у суб'єктів господарювання, які відповідно до положень Закону залучаються до реалізації даного заходу (вказуються в ухвалі суду). Натомість, запропонована редакція цієї норми авторами, у свою чергу, створює можливу ситуацію вимоги від операторів закупівлі та встановлення додаткових засобів. Питання вже врегульовано спеціальним законодавством у сфері електронних комунікацій, зокрема, ст. 121 Закону України «Про електронні комунікації» (набрання чинності, відбудеться 01.01.2022), діючим. Законом України «Про телекомунікації».
…	…	
пункт 5 викласти в такій редакції: "5) витребовувати, збирати і вивчати, за наявності визначених законом підстав, документи та відомості, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, джерела і розміри їх доходів для попередження і припинення розвідувально-підривних, терористичних та інших посягань на державну безпеку; отримувати від операторів та провайдерів телекомунікацій (постачальників	пункт 5 викласти в такій редакції: "5) витребовувати, збирати і вивчати, за наявності визначених законом підстав, документи та відомості, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, джерела і розміри їх доходів для попередження і припинення розвідувально-підривних, терористичних та інших посягань на державну безпеку; отримувати від операторів та провайдерів телекомунікацій (постачальників	Підрозділи та співробітники Служби безпеки України можуть отримувати від операторів та провайдерів телекомунікацій технологічну та іншу інформацію про функціонування мереж, у тому числі з обмеженим доступом, виключно на умовах, визначених володільцем цієї інформації.

електронних комунікаційних послуг та/або мереж) технологічну та іншу інформацію про функціонування мереж, у тому числі з обмеженим доступом, на умовах, визначених володільцем цієї інформації ~~**та підрозділом Служби безпеки України, який уповноважений проводити оперативно-технічні заходи;**~~ брати участь у перевірці походження інвестицій з метою недопущення процесу укладання і реалізації операторами (власниками) об'єктів критичної інфраструктури угод, що можуть негативно вплинути на безпеку, цілісність, стійкість та безперервність функціонування об'єктів критичної інфраструктури, або спроб використання об'єктів критичної інфраструктури у фінансуванні терористичної та розвідувально-підривної діяльності";	електронних комунікаційних послуг та/або мереж) технологічну та іншу інформацію про функціонування мереж, у тому числі з обмеженим доступом, на умовах, визначених володільцем цієї інформації~~;~~ брати участь у перевірці походження інвестицій з метою недопущення процесу укладання і реалізації операторами (власниками) об'єктів критичної інфраструктури угод, що можуть негативно вплинути на безпеку, цілісність, стійкість та безперервність функціонування об'єктів критичної інфраструктури, або спроб використання об'єктів критичної інфраструктури у фінансуванні терористичної та розвідувально-підривної діяльності";	
ж) доповнити новими статтями 8-1 – 8-9 такого змісту:		
Стаття 8-2. Контррозвідувальні заходи, які проводяться за рішенням суду …	Стаття 8-2. Контррозвідувальні заходи, які проводяться за рішенням суду …	
2. Обмеження ~~та/або блокування~~ доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою недопущення терористичного акту або вчинення розвідувально-підривної діяльності на шкоду Україні здійснюється в	2. Обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою недопущення терористичного акту або вчинення розвідувально-підривної діяльності на шкоду Україні, **протидії проведенню**	Пропонується: редакційно уточнити перелік підстав для обмеження доступу з метою приведення у відповідність до повноважень, вказаних у пункті 3^5 ст. 7 законопроекту, адже незрозуміло чому не

судовому порядку на підставі матеріалів кримінального провадження, ~~оперативно-розшукової або контррозвідувальної справи~~. В невідкладних випадках, такий дозвіл може надати уповноважений заступник голови апеляційного суду, в межах територіальної юрисдикції якого перебуває Центральне управління або регіональний орган Служби безпеки України, до складу якого входить відповідний оперативний підрозділ, за клопотанням керівника відповідного оперативного підрозділу Служби безпеки України, що здійснює контррозвідувальну діяльність, або його заступника терміном на ~~7~~ діб. Протягом цього терміну уповноважені посадові особи Служби безпеки України зобов'язані підготувати необхідний перелік документів та звернутися до суду.	**проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації, тих які використовуються для організації, підготовки, вчинення, фінансування, сприяння або приховування акту несанкціонованого втручання в діяльність об'єктів критичної інформаційної інфраструктури** здійснюється в судовому порядку на підставі матеріалів кримінального провадження, оперативно-розшукової або контррозвідувальної справи, **з зазначенням у рішенні суду домену та/або IP-адреси веб-сайту.** В невідкладних випадках, **при провадженні оперативно-розшукової або контррозвідувальної справи, обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) може здійснюватися на підставі дозволу,** який може надати уповноважений заступник голови апеляційного суду, в межах територіальної юрисдикції якого перебуває Центральне управління або регіональний орган Служби безпеки України, до складу якого входить відповідний оперативний підрозділ, за клопотанням керівника відповідного оперативного підрозділу Служби безпеки	для усіх цілей блокування передбачається отримання рішення суду; для правової визначеності дій оператор електронних комунікацій при обмежені доступу до інформаційних ресурсів (сервісів) необхідно зазначити, що у судовому рішенні має бути чітко вказано домен та/або IP-адреси веб-сайту; виключити поняття блокування та залишити тільки обмеження доступу, що не міняє суті характеризується часовими рамками, що і передбачаються в даному пункті. До того ж, доцільно врахувати, що блокування це не функція провайдера. Автоматизувати процес повного блокування/розблокування без відповідного обладнання на сьогодні провайдери не в змозі; термін для подання документів до суду та зібрання доказів пропонується максимально скоротити, так як за цей час оператор несе невиправдані втрати, в т.ч. конкурентні обмеження, споживачі телекомунікаційних послуг не отримують очікуваний перелік контенту, а власник ресурсу несуть фінансово-економічні втрати без належно встановленої винуватості, що можлива лише в судовому порядку; вказати пряму заборону можливого зловживання для безперервного, довготривалого продовження обмеження та/або блокування доступу шляхом

	України, що здійснює контррозвідувальну діяльність, або його заступника терміном на **5** діб. Протягом цього терміну уповноважені посадові особи Служби безпеки України: - **не мають права повторно клопотати про надання дозволу для продовження терміну;** - зобов'язані підготувати необхідний перелік документів і звернутися до суду **та надати оператору, провайдеру телекомунікацій рішення суду про обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів).** **У неотримання такого судового рішення протягом 5 діб з моменту обмеження доступу таке обмеження оператором, провайдером телекомунікацій припиняється.**	отримання нового дозволу після спливу терміну для подачі документів до суду.
…	…	
~~4. У виняткових випадках, коли не вжиття невідкладних заходів призведе до злочину проти основ національної безпеки України, терористичного акту, кібератаки, знищення необхідних фактичних даних або зумовить неможливість їх отримання, Голова Служби безпеки, його заступник або начальник регіонального органу Служби безпеки України має право прийняти документально оформлене рішення щодо проведення~~	**виключити**	

~~контррозвідувальних заходів, передбачених частиною першою цієї статті, до ухвалення рішення суду. У такому випадку керівник оперативного підрозділу Служби безпеки України, яким ініційовано проведення контррозвідувального заходу, або його заступник, повинен протягом 24 годин з початку контррозвідувального заходу звернутися до суду з клопотанням про надання дозволу на проведення контррозвідувальних заходів. Окрім відомостей, передбачених статтею 8-3 цього Закону, у клопотанні мають зазначатися обставини, які зумовили необхідність невідкладного проведення відповідного контррозвідувального заходу.~~ ~~Якщо за результатами розгляду клопотання в порядку, передбаченому статтею 8-3 цього Закону, судом постановлено ухвалу про відмову у наданні дозволу на проведення контррозвідувального заходу, контррозвідувальний захід підлягає негайному припиненню, а одержана внаслідок його проведення інформація передається оперативному підрозділу-ініціатору проведення контррозвідувального заходу для знищення у встановленому порядку.~~		
~~16) у Законі України "Про телекомунікації" (Відомості Верховної~~	**виключити**	на підставі ч. 2 роздізу XIX. ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ Закону України «Про

~~Ради України, 2004 р., № 12, ст. 155 із наступними змінами):~~ ~~а) частину першу статті 24 доповнити абзацом такого змісту:~~ ~~"Технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації, що встановлюються для здійснення відповідними органами оперативно-розшукових та контррозвідувальних заходів, повинні відповідати стандартам і технічним регламентам, які розробляє уповноважений на це законом державний орган";~~		електронні комунікації».