Додаток до листа Телекомпалати України від 24.06.2021 №2607

ПОРІВНЯЛЬНА ТАБЛИЦЯ

пропозицій та зауважень Асоціації «Телекомунікаційна палата України» до проекту Закону України «Про Службу безпеки України» реєстраційний номер 3196-д

--

Запропонована редакція 3196-д	Редакція з врахуванням пропозицій Асоціації	Коментарі
Закон України	Закон України	
Про Службу безпеки України	Про Службу безпеки України	
РОЗДІЛ III	РОЗДІЛ III	
ПОВНОВАЖЕННЯ ТА ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІСЛУЖБИ БЕЗПЕКИ УКРАЇНИ	ПОВНОВАЖЕННЯ ТА ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІСЛУЖБИ БЕЗПЕКИ УКРАЇНИ	
Стаття 11. Повноваження Служби безпеки України	Стаття 11. Повноваження Служби безпеки України	
1. Служба безпеки України, її органи, відповідні підрозділи, заклади (підрозділи закладів), установи та співробітники з метою виконання покладених завдань при здійсненні визначених цим Законом функцій в межах компетенції уповноважені:	Служба безпеки України, її органи, відповідні підрозділи, заклади (підрозділи закладів), установи та співробітники з метою виконання покладених завдань при здійсненні визначених цим Законом функцій в межах компетенції уповноважені:	
….	…	
7) здійснювати на підставі рішення суду тимчасове обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою недопущення терористичного акту або вчинення розвідувально-підривної діяльності на шкоду Україні, протидії проведенню проти України спеціальних	7) здійснювати на підставі рішення суду тимчасове обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою недопущеннятерористичного акту або вчинення розвідувально-підривної діяльності на шкоду Україні, протидії проведенню проти України спеціальних	

інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, тих які використовуються для організації, підготовки, вчинення, фінансування, сприяння або приховування акту несанкціонованого втручання в	інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, 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, у порядку встановленому законом, брати участь у застосуванні санкцій на виконання рішень Ради національної безпеки і оборони України;	діяльність об'єктів критичної інформаційної інфраструктури, ~~з використанням технічних засобів, що встановлюються операторами, провайдерами телекомунікацій та іншими суб'єктами господарювання~~, у порядку встановленому законом, брати участь у застосуванні санкцій на виконання рішень Ради національної безпеки і оборони України;	Зайве уточнення, яке породжує двозначне тлумачення, що нібито оператори зобов'язані придбавати якесь додаткове обладнання.
Стаття 13. Збирання та отримання інформації Службою безпеки України	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 закону здійснюється збирання та отримання інформації, у тому числі персональних даних, шляхом:	1. Для забезпечення виконання покладених на Службу безпеки України завдань її силами та засобами відповідно до закону здійснюється збирання та отримання інформації, у тому числі персональних даних, шляхом:	
здійснення моніторингу джерел інформації, а також інших заходів, спрямованих на збирання інформації;	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;~~	отримання у встановленому порядку на безоплатній основі інформації від правоохоронних та інших державних органів, військових формувань, органів місцевого самоврядування.	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.
…	…	
відсутній	**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 Головою Служби безпеки України, його заступником, 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 повинен невідкладно у письмовій формі повідомити про це підрозділ Служби безпеки	2.Отримання Службою безпеки України інформації може здійснюватися на підставі запиту, підписаного Головою Служби безпеки України, його заступником, 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	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.

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.**~~	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	
3. Для отримання інформації Служба безпеки України може використовувати:спеціальні методи і засоби збирання інформації, у тому числі спеціальні технічнізасоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації; прямий доступ до автоматизованих інформаційних, довідкових систем, обліків, реєстрів, банків або баз даних, держателем (адміністратором) яких є правоохоронні, державні органи, органи місцевого самоврядування, підприємства, установи та організації будь-якої форми власності, а також одержувати від них копії інформаційних фондів зазначених систем з їх оновленням у режимі реального часу. Порядок доступу Служби безпеки України до автоматизованих інформаційних, довідкових систем, обліків, реєстрів, банків або баз даних, документів, інших матеріальних носіїв інформації правоохоронних та розвідувальних органів України, ~~**а також взаємодія з інших питань визначається спільними актами Служби безпеки України та таких органів.**~~	3.Для отримання інформації Служба безпеки України може використовувати: спеціальні методи і засоби збирання інформації, у тому числі спеціальні технічнізасоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації; прямий доступ до автоматизованих інформаційних, довідкових систем, обліків, реєстрів, банків або баз даних, держателем (адміністратором) яких є правоохоронні, державні органи, органи місцевого самоврядування, підприємства, установи та організації будь-якої форми власності, а також одержувати від них копії інформаційних фондів зазначених систем з їх оновленням у режимі реального часу. Порядок доступу Служби безпеки України до автоматизованих інформаційних, довідкових систем, обліків, реєстрів, банків або баз даних, документів, інших матеріальних носіїв інформації правоохоронних та розвідувальних органів України, **виключно за рішенням суду.**	Ця норма має бути доповнена положеннями про те, що СБУ має право у встановленому порядку та виключно на підставі рішення суду отримувати інформацію, яка містить комерційну та банківську таємницю, персональні дані фізичної особи від підприємств, установ, організацій та фізичних осіб; Норма про прямий доступ до автоматизованих інформаційних, довідкових систем, обліків, реєстрів, банків або баз даних приватних компаній повинна бути змінена. З цієї норми повинні бути виключені приватні компанії або визначений (регламентований) чіткий порядок взаємодії між СБУ та підприємствами, установами, організаціями недержавної власності.
4. В інтересах національної безпеки, з метою попередження та припинення посягань на державний суверенітет, конституційний лад і територіальну цілісність України, злочинів проти миру та безпеки людства, протидії тероризму та	4.В інтересах національної безпеки, з метою попередження та припинення посяганьна державний суверенітет, конституційний лад і територіальну цілісність України, злочинів проти миру та безпеки людства,	

розвідувально- підривної діяльності, захисту прав і свобод інших осіб, Служба безпеки України також може отримувати:	протидії тероризму та розвідувально-підривної діяльності, захисту прав і свобод інших осіб, 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;	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 **виключно за рішенням суду;**	Приведення у відповідність до вимог статті 121 Закону України «Про електронні комунікації» 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) 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 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.		
5. З метою встановлення ідентичності осіб або отримання у невідкладних випадках інших необхідних для виконання покладених на неї завдань даних Служба безпеки України має право ~~**на підставі запиту, оформленого відповідно до частини другої цієї статті,**~~ одержувати безпосередній доступ до стаціонарних та рухомих систем і приладів радіоконтролю, аудіо, відео та аудіо/відео спостереження, а також відповідних матеріальних носіїв інформації, що належать фізичним особам та/або підприємствам, установам, організаціям недержавної форми власності – за їх згодою чи з дозволу суду, якщо законом передбачено надання такого дозволу.	5.З метою встановлення ідентичності осіб або отримання у невідкладних випадках інших необхідних для виконання покладених на неї завдань даних Служба безпеки України має право одержувати безпосередній доступ до стаціонарних та рухомих систем і приладів радіоконтролю, аудіо, відео та аудіо/відео спостереження, а також відповідних матеріальних носіїв інформації, що належать фізичним особам та/абопідприємствам, установам, організаціям недержавної форми власності – за їх згодою чи з дозволу суду, якщо законом передбачено надання такого дозволу.	Положення цієї статті щодо прямого доступу СБУ до інформаційних ресурсів та отримання копій інформаційних фондів потребує редагування з метою недопущення порушення гарантованих Конституцією України прав і свобод громадян, а також несанкціонованого доступу до конфіденційної інформації про особу та незаконного поширення такої інформації.
…	…	
…	…	
II. Прикінцеві та перехідні положення	II. Прикінцеві та перехідні положення	
14. Внести зміни до таких законодавчих актів України:	Внести зміни до таких законодавчих актів України:	
16) у Законі України "Про контррозвідувальну діяльність" (Відомості Верховної Ради України, 2003 р., № 12, ст. 89 із наступними змінами):	16) у Законі України "Про контррозвідувальну діяльність" (Відомості Верховної Ради України, 2003 р., № 12, ст. 89 із наступними змінами):	
…	…	
е) у статті 7:	е) у статті 7:	
у частині другій:	у частині другій:	
пункт 3 замінити пунктами такого змісту:	пункт 3 замінити пунктами такого змісту:	
“3) проводити контррозвідувальні та спеціальні інформаційні операції, контррозвідувальне впровадження;	“3) проводити контррозвідувальні та спеціальні інформаційні операції, контррозвідувальне впровадження;	
…	…	

3-5) здійснювати на підставі рішення суду тимчасове обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою недопущення терористичного акту або вчинення 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;~~	3-5) здійснювати на підставі рішення суду тимчасове обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою недопущення терористичного акту або вчинення 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.	Створює можливу ситуацію вимоги від операторів, провайдерів закупівлі та встановлення додаткових технічних засобів. Такі заходи можуть бути вжиті в ході контррозвідувальної діяльності органами, підрозділами та співробітниками Служби 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). Ця норма створює необгрунтовану можливість вимоги від операторів, провайдерів телекомунікацій закупівлі та встановлення додаткових технічних засобів. Крім цього, першою ланкою обмеження доступу до певного ресурсу є володілець цього ресурсу, а не оператор, провайдер телекомунікацій, який відповідно до спеціального закону не несе відповідальність за зміст інформації, що передається його мережами. У зв'язку із цим, виокремлення операторів, провайдерів може призвести до необґрунтованого надмірного навантаження у першу чергу саме цих суб'єктів господарювання в частині виконання невластивих бізнесу функцій.
пункт 5 викласти в такій редакції:	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	5) витребовувати, збирати і вивчати, за наявності визначених законом підстав, документи та відомості, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих	Приведення у відповідність до вимог статті 121 Закону України «Про електронні комунікації». Крім цього, підрозділи та співробітники Служби безпеки України

припинення розвідувально-підривних, терористичних та інших посягань на державну безпеку; отримувати від операторів та провайдерів телекомунікацій (постачальників 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 недопущенняпроцесу 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";	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 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 **виключно за рішенням суду ~~та підрозділом Служби безпеки України, який уповноважений проводити оперативно- технічні заходи~~**; брати участь у перевірці походження інвестицій з метою недопущенняпроцесу 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";	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.
пункт 6 викласти у такій редакції:	пункт 6 викласти у такій редакції:	
ж) доповнити новими статтями 8^1 – 8^9 такого змісту:	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 …	
1. Виключно з метою попередження, своєчасного виявлення і припинення розвідувальних, підривних, терористичних та інших посягань на державну безпеку України, отримання інформації в		

інтересах державної безпеки України органи, підрозділи та співробітники Служби безпеки України мають право здійснювати за рішенням суду такі контррозвідувальні заходи:		
а) спостереження за особою або місцем із фіксацією відповідних відомостей або даних;		
б) аудіо-, відеоконтроль особи, що полягає у втручанні в приватне спілкування особибез її відома з фіксацією змісту її розмов або інших звуків, рухів, дій, пов'язаних з її діяльністю або місцем перебування тощо за допомогою аудіо, відеозапису із використанням спеціальних та інших технічних засобів;		
в) аудіо-, відео контроль місця, що полягає у здійсненні прихованої фіксації відомостей за допомогою аудіо-, відеозапису всередині публічно доступних місць, без відома їх власника, володільця або присутніх у цьому місці осіб;		
г) зняття інформації з телекомунікаційних мереж (транспортних телекомунікаційних мереж, що забезпечують передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду між підключеними до неї телекомунікаційними мережами доступу);		
ґ) зняття інформації з електронних інформаційних мереж, яке полягає у пошуку, виявленні шляхом фізичного та/або програмного доступу, відборі і фіксації відомостей або даних, що містяться в електронних інформаційних мережах (системах) або її частинах, доступ до яких обмежується її власником, володільцем, утримувачем або пов'язаний з подоланням системи логічного захисту;		
д) обстеження публічно недоступних місць, житла чи іншого володіння особи, шляхом негласного проникнення до таких місць, житла чи володіння		

особи з використанням спеціальних та інших технічних засобів, з метою:		
виявлення і фіксації речей і документів;		
виготовлення копій чи зразків зазначених речей і документів, виявлення тавилучення зразків для дослідження;		
виявлення осіб, які можуть бути причетні до розвідувально-підривній діяльності,терористичним та іншим протиправним посяганням на державну безпеку України;		
встановлення технічних засобів аудіо-, відеоконтролю особи;		
є) установлення місцезнаходження радіоелектронного засобу, яке полягає в локалізації місцезнаходження радіоелектронного засобу, в тому числі мобільного терміналу систем зв'язку, та інших радіовипромінювальних пристроїв, активованих у мережах операторів, провайдерів телекомунікацій, без розкриття змісту повідомлень, що передаються;		
е) огляд кореспонденції, який полягає в негласному відборі за ідентифікаційними ознаками кореспонденції, її обробленні, зміні (заміні), знятті копій чи отриманні зразків.		
2. Обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів(сервісів) з метою недопущення терористичного акту або вчинення розвідувально- підривної діяльності на шкоду Україні здійснюється в судовому порядку на підставі матеріалів кримінального провадження, оперативно-розшукової або контррозвідувальної справи.	2. Обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів) з метою недопущення терористичного акту або вчинення 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**	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 для усіх цілей блокування передбачається отримання рішення суду;

	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	
…	…	
~~3. У виняткових випадках, коли невжиття 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 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.~~	**виключити**	Виключно на підставі рішення суду, без будь яких окремих випадків має відбуватися будь-який контррозвідувальний захід щодо фізичних чи юридичних осіб.
~~Якщо за результатами розгляду клопотання в порядку, передбаченому статтею 8-3 цього Закону,~~		

~~судом постановлено ухвалу про відмову у наданні дозволу на проведенняконтррозвідувального заходу, контррозвідувальний захід підлягає негайному припиненню, а одержана внаслідок його проведення інформація передається оперативному підрозділу-ініціатору проведення контррозвідувального заходу для знищення у встановленому порядку.~~		
…		