**Додаток до Вих. № 89/1-4 від 24.05.2021**

**ПОРІВНЯЛЬНА ТАБЛИЦЯ**

**із зауваженнями та пропозиціями ІнАУ до проекту Закону про внесення змін до Закону України "Про Службу безпеки України" щодо удосконалення організаційно-правових засад діяльності Служби безпеки України**

| **Положення у тексті проекту Закону** | **Положення до проекту Закону, запропоновані ІнАУ** | **Обґрунтування пропозицій ІнАУ** |
|---|---|---|
| **Проект Закону «Про Службу безпеки України» (в новій редакції)** | | |
| Стаття 11. Повноваження Служби безпеки України<br>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:<br>… | Стаття 11. Повноваження Служби безпеки України<br>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:<br>… | |
| 14) **проводити спеціальні інформаційні операції**, протидіяти проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації;<br>… | 14) **проводити спеціальні інформаційні операції,** протидіяти проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації;<br>… | **<u>Коментар:</u>** У цьому ЗП не надається визначення терміну «інформаційна операція», «спеціальна інформаційна операція». Проте, розробниками надається визначення терміну «спеціальна інформаційна операція» у змінах до ЗУ «Про контррозвідку», яке є нечітким.<br>**<u>ПРОПОЗИЦІЯ:</u>** Доопрацювати поняття «спеціальні інформаційні операції» з метою його чіткості та лаконічності та надати саме у ЗП про СБУ. |
| 27) брати участь у перевірці та оцінці захищеності об’єктів критичної інфраструктури, протидії актам несанкціонованого втручання в діяльність об’єктів критичної інфраструктури; | 27) брати участь у перевірці та оцінці захищеності об’єктів критичної інфраструктури, протидії актам несанкціонованого втручання в діяльність об’єктів критичної інфраструктури **у порядку, встановленому законодавством;** | **<u>Коментар:</u>** виконання органами СБУ дій повинно відбуватись в межах порядку, встановленого у законі, а не довільно. |

| | | |
|---|---|---|
| Стаття 13. Збирання та отримання інформації Службою безпеки України<br>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:<br>… | Стаття 13. Збирання та отримання інформації Службою безпеки України<br>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:<br>… | **Коментар:** пропонуємо слово «законодавством» замінити словом «закону», адже збір, поширення інформації про персональні дані регулюється саме законами, зокрема, Конституцією України, Законом України «Про захист персональних даних» тощо. Збір інформації, наявної у операторів, провайдерів телекомунікацій, іншої охоронюваної законом інформації також регулюється законом, а не законодавством, що розуміє в собі і нормативно-правові акти. |
| 3. Для отримання інформації Служба безпеки України може використовувати:<br>спеціальні ~~методи і~~ засоби збирання інформації, у тому числі спеціальні технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації;<br>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.<br>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 | 3. Для отримання інформації Служба безпеки України може використовувати:<br>**спеціальні засоби** збирання інформації, у тому числі спеціальні технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації;<br>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.<br>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 | **Коментар:** Що таке «спеціальні методи»? законом та іншим законодавством не визначено. Може мати наслідком порушення прав підприємств та громадян. Тому, пропонується вилучити слова «методи і»<br><br>**Коментар:** Із запропонованого формулювання не зрозуміло, які це - «таких» органів»? Тобто, йдеться лише про правоохоронні та розвідувальні органи та їх ресурси чи, з урахуванням попереднього положення, усіх органів влади підприємств тощо. Чому не |

| | | |
|---|---|---|
| питань визначається спільними актами Служби безпеки України та таких органів. | питань визначається спільними актами Служби безпеки України та таких органів, **які погоджуються з Адміністрацією ДССЗЗІ.** | згадується про ДССЗЗІ та НКРЗІ?<br>Тому, запропонована уточнена редакція положення. |
| **Відсутній** | **Конфіденційну інформацію, персональні дані фізичної особи, інформацію, яка знаходиться в операторів та провайдерів телекомунікацій та іншу охоронювану законами України інформацію Служба безпеки України має право отримувати у встановленому законами порядку та виключно на підставі рішення суду, ухвали слідчого судді.** | **Коментар:** З метою дотримання співробітниками СБУ Конституції України та інших законів щодо захисту конфіденційної інформації, захисту персональних даних, пропонується новий абзац. |
| 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:<br>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; | 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:<br>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; | |
| **Відсутній** | **Отримання інформації від операторів та провайдерів телекомунікацій здійснюється на підставі, в межах повноважень та у спосіб, що передбачені Конституцією України та законами України «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», Кримінальним процесуальним кодексом України, іншими законами України.** | **Коментар:** Оскільки у проекті Закону не встановлено перелік випадків та процедур використання спеціальних методів і засобів збирання інформації, у тому числі з використанням спеціальних технічні засоби для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, з метою недопущення порушення прав фізичних осіб, а також операторів, |

| | | |
|---|---|---|
| 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.<br>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. | **Інформація про абонента та/або отримані електронні комунікаційні послуги надається лише на підставі рішення суду або за наявності попередньої згоди абонента, вираженої у письмовій або будь-якій іншій формі, що дає змогу зробити висновок про факт надання ним згоди.**<br>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.<br>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. | провайдерів телекомунікацій пропонується уточнити, що виконання таких дій повинно відбуватись виключно відповідно та в межах Конституції та законів України. |
| **Закон України «Про контррозвідувальну діяльність»** | | |
| у статті 7:<br>…<br>3-1) здійснювати контррозвідувальне опитування осіб, які мають допуск до державної, розвідувальної таємниці та/або у зв'язку з їх допуском до державної, розвідувальної таємниці, дипломатичних та адміністративних службовців Міністерства закордонних справ, які відряджаються, знаходяться або повертаються з довготермінового відрядження, військовослужбовців, осіб, які працюють з ядерними матеріалами та на ядерних установках, а також осіб, які працюють на об'єктах критичної інфраструктури та у інших передбачених | у статті 7:<br>…<br>3-1) здійснювати контррозвідувальне опитування осіб, які мають допуск до державної, розвідувальної таємниці та/або у зв'язку з їх допуском до державної, розвідувальної таємниці, дипломатичних та адміністративних службовців Міністерства закордонних справ, які відряджаються, знаходяться або повертаються з довготермінового відрядження, військовослужбовців, осіб, які працюють з ядерними матеріалами та на ядерних установках, а також осіб, які працюють на | **Коментар:** Пропонуємо, щоб не лише випадки, а і порядки, визначались законом. |

| | | |
|---|---|---|
| законодавством випадках;<br><br>…<br>3-5) здійснювати тимчасове обмеження доступу до визначених (ідентифікованих) 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, що встановлюються операторами, провайдерами телекомунікацій та іншими суб'єктами господарювання;<br><br>…<br><br>пункт 5 викласти в такій редакції:<br>"5) витребовувати, збирати і вивчати, за наявності визначених законом підстав, документи та відомості, що характеризують | об'єктах критичної інфраструктури та у інших передбачених законодавством випадках **та у порядку, встановленому законом;**<br>**…**<br>**3-5) на підставі рішення суду вимагати від володільців визначених (ідентифікованих) інформаційних ресурсів (сервісів) або від дата-центрів де розміщуються ці сервіси (ресурси), обмеження доступу до цих 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, тих, які використовуються для організації, підготовки, вчинення, фінансування, сприяння або приховування акту несанкціонованого втручання в діяльність об'єктів критичної інформаційної інфраструктури у порядку, встановленому законом;**<br><br>…<br><br>пункт 5 викласти в такій редакції:<br>"5) витребовувати, збирати і вивчати, за наявності визначених законом підстав, документи та відомості, що характеризують діяльність підприємств, установ, організацій, а | **Коментар:** з метою недопущення порушення конституційних прав громадян, а також прав та законних інтересів юридичних осіб, виключно на підставі рішення суду може здійснюватись обмеження доступу до визначених (ідентифікованих) інформаційних ресурсів (сервісів).<br>Технічно блокування і видалення інтернет-контенту можливе лише в разі його виконання володільцем вебсайту або дата-центром, де розміщений цей контент. Коректне блокування інтернет-контенту провайдерами доступу технічно неможливе, про що свідчить також негативний вітчизняний досвід спроб впровадження блокування на доступі з 2017 року.<br>Крім того, це положення у проекті Закону сформовано з недотриманням гарантованого Конституцією України права власності. Адже телекомунікаційні мережі, є приватною власністю. Натомість, з сформульованого положення виходить так, що органам СБУ власник зобов'язаний надати безмежне та поза законом право керування (управління, розпорядження) телекомунікаційними мережами<br><br>**Коментар:** відповідно до частини другої статті 11 Закону України «Про інформацію» не допускаються збирання, зберігання, використання та поширення конфіденційної |

| | | |
|---|---|---|
| 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 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";<br>…<br>Стаття 8-2. Контррозвідувальні заходи, які проводяться за рішенням суду<br>1. Виключно з метою попередження, своєчасного виявлення і припинення розвідувально-підривних, терористичних та інших посягань на державну безпеку, отримання інформації в інтересах державної безпеки органи, підрозділи та співробітники Служби безпеки України мають право здійснювати за рішенням суду такі контррозвідувальні заходи: | 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 технологічну інформацію про функціонування мереж, у тому числі з обмеженим доступом, на умовах, визначених володільцем цієї інформації та законами України, а також іншу інформацію на умовах, встановлених Конституцією та законами України;** 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";<br>…<br>Стаття 8-2. Контррозвідувальні заходи, які проводяться за рішенням суду<br>1. Виключно з метою попередження, своєчасного виявлення і припинення розвідувально-підривних, терористичних та інших посягань на державну безпеку, отримання інформації в інтересах державної безпеки органи, підрозділи та співробітники Служби безпеки України мають право здійснювати за рішенням суду такі контррозвідувальні заходи: | інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. Відповідно до частини другої статті 21 Закону України «Про інформацію» конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.<br>Оскільки телекомунікаційні мережі є власністю оператора, провайдера телекомунікацій, то лише ці суб'єкти, як це встановлено законом, можуть визначати умови поширення інформації про функціонування телекомунікаційних мереж. В інших випадках, така інформація може бути надана виключно на підставі рішення суду, ухвали слідчого судді. |

| | | |
|---|---|---|
| …<br>г) зняття інформації з телекомунікаційних мереж (мереж, що забезпечують передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду між підключеними до неї телекомунікаційними мережами доступу);<br>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;<br>**Відсутній** | …<br>**г) зняття інформації з телекомунікаційних мереж, електронних інформаційних систем, або їх частин, яке полягає у проведенні із застосуванням відповідних технічних засобів, відбору та фіксації змісту інформації або даних, без відома її власника, володільця або утримувача;**<br>**Порядок встановлення, технічного обслуговування таких технічних засобів, права та обов'язки операторів, провайдерів телекомунікацій при підключенні до своїх телекомунікаційних мереж технічних засобів для здійснення оперативно-розшукових та розвідувальних заходів та забезпеченні їх функціонування визначаються законом у сфері телекомунікацій.** | **Коментар:** пропонується уточнена редакція до підпункту г). |
| ….<br>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 судовому порядку на підставі матеріалів кримінального провадження, оперативно-розшукової або контррозвідувальної справи. В невідкладних випадках, такий дозвіл | …<br>**2. З метою недопущення терористичного акту або вчинення розвідувально-підривної діяльності на шкоду Україні в судовому порядку на підставі матеріалів кримінального провадження, оперативно-розшукової або контррозвідувальної справи вимагати від володільців ресурсів або датацентрів, де ці ресурси розміщені, блокувати або видаляти визначені** | **Коментар:** Технічно блокування і видалення інтернетконтенту можливе лише в разі його виконання володільцем вебсайту або дата-центром, де розміщений цей контент. Коректне блокування інтернет-контенту провайдерами доступу технічно неможливе, про що свідчить також негативний вітчизняний досвід спроб впровадження блокування на доступі з 2017 року. |

| | | |
|---|---|---|
| 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. | **(ідентифіковані) в цьому впровадженні ресурси (сервіси).** | |
| … | … | |
| Стаття 8-3. Особливості розгляду судом клопотань про надання дозволу на проведення контррозвідувальних заходів | Стаття 8-3. Особливості розгляду судом клопотань про надання дозволу на проведення контррозвідувальних заходів | |
| … | … | |
| У клопотанні про надання дозволу на проведення контррозвідувальних заходів, визначених частиною першою статті 82 цього Закону, зазначаються: | У клопотанні про надання дозволу на проведення контррозвідувальних заходів, визначених частиною першою статті 82 цього Закону, зазначаються: | |
| … | … | |
| 7) найменування оператора (за необхідності), провайдера телекомунікацій або власника (володільця) кабельної каналізації електрозв'язку, сприяння якого є необхідним для організації та проведення контррозвідувального заходу. | 7) найменування оператора (за необхідності), провайдера телекомунікацій або власника (володільця) кабельної каналізації електрозв'язку, сприяння якого є необхідним для організації та проведення контррозвідувального заходу. | |
| Клопотання про надання дозволу на проведення контррозвідувальних заходів, визначених частиною першою статті 82 цього Закону, передається уповноваженому заступнику голови апеляційного суду та реєструється з дотриманням | Клопотання про надання дозволу на проведення контррозвідувальних заходів, визначених частиною першою статті 82 цього Закону, передається уповноваженому заступнику голови | |

| | | |
|---|---|---|
| вимог законодавства про охорону державної таємниці.<br><br>**Відсутній**<br><br>**…**<br>Ухвала про надання дозволу на проведення контррозвідувального заходу, визначеного частиною першою статті 82 цього Закону, повинна містити:<br>**…**<br>4) вимогу до оператора, провайдера телекомунікацій або власника (володільця) кабельної каналізації електрозв'язку (з зазначенням їх найменування) про надання сприяння в організації та проведенні контррозвідувального заходу (за необхідності);<br><br>**…**<br><br>Стаття 8-5. Офіційне застереження<br>Офіційне застереження – роз'яснення Службою безпеки України фізичній чи юридичній особі про те, що її діяння (дія або бездіяльність) створює умови для виникнення чи реалізації загроз державній безпеці або підвищує ризики державної безпеки, а відтак є неприпустимим.<br>Офіційне застереження здійснюється у формі письмового інформування після проведення | апеляційного суду та реєструється з дотриманням вимог законодавства про охорону державної таємниці.<br>**Клопотання повинно містити перелік дій та їх опис, які повинен вжити оператор, провайдер телекомунікацій для забезпечення можливості проведення контррозвідувального заходу.**<br>**…**<br>Ухвала про надання дозволу на проведення контррозвідувального заходу, визначеного частиною першою статті 82 цього Закону, повинна містити:<br>…<br>4) вимогу до оператора, провайдера телекомунікацій або власника (володільця) кабельної каналізації електрозв'язку (з зазначенням їх найменування) про надання сприяння в організації та проведенні контррозвідувального заходу (за необхідності) **з зазначенням конкретних дій та заходів, яких повинен вжити оператор, провайдер телекомунікацій або власник (володілець) кабельної каналізації електрозв'язку;**<br>**…**<br><br>**Виключити** | **<u>Коментар:</u>** Оскільки законодавством не встановлено чіткого переліку заходів та дій, які повинен виконати оператор, провайдер телекомунікацій, з метою недопущення порушення прав, свобод та законних інтересів третіх осіб, необхідно, щоб саме суд у своєму рішенні (ухвалі) вказав чіткий перелік таких заходів та дій, які повинен здійснити оператор, провайдер телекомунікацій для сприяння в організації та проведенні контррозвідувального заходу.<br><br>**<u>Коментар:</u>** Пропонується виключити із тексту законопроекту цю статтю, оскільки, такого поняття та документу «офіційне застереження» в Україні немає, відсутні механізми його оскарження, в т.ч. й до суду.<br>Цією статтею такі механізми також не запропоновані. Крім того, не запропоновані чіткі критерії, коли такі документи можуть бути винесені, процедура їх винесення, |

| | | |
|---|---|---|
| Службою безпеки України перевірки та підтвердження отриманих у ході оперативно-службової діяльності відомостей про фізичну або юридичну особу.<br>Право підписання офіційного застереження належить Голові Служби безпеки України, його заступникам, начальникам регіональних органів Служби безпеки України, їх заступникам.<br>Офіційне застереження адресується конкретній фізичній особі або керівнику (уповноваженій відповідальній посадовій особі) юридичної особи і повинне містити:<br>1) зазначення діяльності, що створює умови для реалізації загроз державній безпеці або підвищує ризики державної безпеки, щодо неприпустимості здійснення якого фізична або юридична особа застерігається;<br>2) роз'яснення права оскарження офіційного застереження до вищої посадової особи Служби безпеки України або до суду. | | реагування та докази виконання юридичною чи фізичною особою тощо.<br>Відсутність таких положень закладає, на наш погляд корупційну складову, коли співробітники СБУ на власний розсуд будуть користуватись таким правом.<br>Крім того, за юридичним визначенням застереження не може бути роз'ясненням. Це може бути документ обов'язкового або рекомендаційного характеру. Проте, у тексті статті про це не зазначається. Тобто, пропонується, що СБУ буде забороняти здійснювати певну діяльність для певного суб'єкта. І це буде відбуватись без рішення суду. |
| ….<br>Стаття 8-7. Контрольоване використання майна, вилученого чи обмеженого у цивільному обороті<br>При здійсненні контррозвідувальної діяльності співробітники Служби безпеки України, а також особи, залучені до конфіденційного співробітництва, з дозволу Голови Служби безпеки України або уповноважених ним керівників можуть придбавати, зберігати, переміщувати, реалізовувати вилучене з обороту чи обмежене у цивільному обороті майно, в тому числі те, яке не може перебувати у власності громадян, громадських об'єднань, міжнародних організацій та юридичних осіб інших держав на території України. | …<br>Стаття 8-7. Контрольоване використання майна, вилученого чи обмеженого у цивільному обороті<br>При здійсненні контррозвідувальної діяльності співробітники Служби безпеки України, а також особи, залучені до конфіденційного співробітництва, з дозволу Голови Служби безпеки України або уповноважених ним керівників можуть придбавати, зберігати, переміщувати, реалізовувати вилучене з обороту чи обмежене у цивільному обороті майно, в тому числі те, яке не може перебувати у власності громадян, громадських об'єднань, міжнародних організацій та юридичних осіб | **<u>Коментар:</u>** Пропонується, щоб саме Кабінет Міністрів України своїми постановами визначав порядок контролю за придбанням, зберіганням, переміщенням, реалізацією майна, вилученого чи обмеженого у цивільному обороті. |

| | | |
|---|---|---|
| Порядок контролю за придбанням, зберіганням, переміщенням, реалізацією майна, зазначеного в частині першій цієї статті, визначається ~~нормативно-правовими актами Служби безпеки України, погодженими з центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сферах боротьби зі злочинністю, виявлення кримінальних правопорушень, охорони громадського порядку та забезпечення громадської безпеки.~~ | інших держав на території України.<br>Порядок контролю за придбанням, зберіганням, переміщенням, реалізацією майна, зазначеного в частині першій цієї статті, визначається **Кабінетом Міністрів України.** | |
| **Закон України «Про телекомунікації»** | | |
| у Законі України "Про телекомунікації" (Відомості Верховної Ради України, 2004 р., № 12, ст. 155 із наступними змінами):<br>а) частину першу статті 24 доповнити абзацом такого змісту:<br>"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"; | **Виключити** | **<u>Коментар:</u>** Основним обов’язком операторів, провайдерів телекомунікацій є задоволення потреб споживачів (абонентів) телекомунікаційними послугами достатнього асортименту, обсягу та якості відповідно до законодавства у сфері телекомунікацій. Оператори, провайдери телекомунікацій не виконують, не мають та не можуть мати жодного відношення до здійснення відповідними органами оперативно-розшукових та контррозвідувальних заходів. Відтак, цими доповненнями до Закону пропонується встановити операторам, провайдерам телекомунікацій не властиві для них функції та повноваження.<br>Для надання телекомунікаційних послуг не використовуються технічні засоби для зняття інформації, тому, зазначене доповнення до статті 24 Закону, що регулює діяльність операторів, провайдерів телекомунікацій, необґрунтоване. |