КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 4 червня 2025 р. № 669

Київ

Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України

Кабінет Міністрів України **постановляє**:

Внести до Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 р. № 411 (Офіційний вісник України, 2014 р., № 73, ст. 2066; 2018 р., № 31, ст. 1090; 2023 р., № 26, ст. 1474, № 65, ст. 3712; 2024 р., № 83, ст. 4951), зміни, що додаються.

Прем’єр-міністр України **Д. ШМИГАЛЬ**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 4 червня 2025 р. № 669

ЗМІНИ,
що вносяться до Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України

1. Пункт 1 після абзацу п’ятого доповнити абзацами такого змісту:

“центральним органом виконавчої влади, який забезпечує здійснення Держспецзв’язку повноважень уповноваженого органу, що забезпечує функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

центральним органом виконавчої влади, який забезпечує здійснення Держспецзв’язку повноважень уповноваженого органу, що забезпечує функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;”.

У зв’язку з цим абзац шостий вважати абзацом восьмим.

2. У пункті 4:

1) підпункт 11 викласти в такій редакції:

“11) забезпечує функціонування державної системи урядового зв’язку, її безпеки, розвитку та готовності до роботи в особливий період і в разі виникнення надзвичайної ситуації;”;

2) доповнити пункт підпунктами 15^2 і 15^3 такого змісту:

“15^2) забезпечує здійснення Держспецзв’язку передбачених Законом України “Про основні засади забезпечення кібербезпеки України” повноважень уповноваженого органу, що забезпечує функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

15^3) забезпечує здійснення Держспецзв’язку передбачених Законом України “Про основні засади забезпечення кібербезпеки України” повноважень уповноваженого органу, що забезпечує функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;”;

3) абзац п’ятий підпункту 16 після слів “ключових документів” доповнити словами “та державних шифрів”;

4) підпункти 17 та 42 викласти в такій редакції:

“17) установлює порядок організації та проведення державної експертизи у сфері криптографічного та технічного захисту інформації, забезпечує організацію проведення державної експертизи щодо відсутності

у програмному забезпеченні недокументованих функцій, проводить експертні та тематичні дослідження у сфері криптографічного захисту інформації, визначає криптографічні алгоритми як рекомендовані, надає допуск до експлуатації засобів криптографічного захисту інформації, видає експертні висновки за результатами державної експертизи у сфері криптографічного захисту інформації, свідоцтва про допуск до експлуатації засобів криптографічного захисту інформації, реєструє експертні висновки за результатами державної експертизи у сфері технічного захисту інформації, декларації та атестати відповідності комплексних систем захисту інформації;";

"42) установлює:

технічні вимоги до електронних комунікаційних мереж та об'єктів спеціального зв'язку;

порядок і забезпечує проведення експертизи інфраструктури електронних комунікацій проектів будівництва, реконструкції та модернізації електронних комунікаційних мереж, споруд спеціального зв'язку;";

5) доповнити пункт підпунктом 42^1 такого змісту:

"42^1) затверджує до використання переліки стандартів, настанов, рекомендацій, аналітичних оглядів та інших документів, розроблених та прийнятих іноземними та міжнародними організаціями з питань, що належать до повноважень Держспецзв'язку, в тому числі документів Міжнародної організації зі стандартизації (ISO), Європейського комітету зі стандартизації (CEN), Європейського інституту телекомунікаційних стандартів (ETSI), Міжнародного союзу електрозв'язку (ITU), Агентства Європейського Союзу з кібербезпеки (ENISA), Агентства з кібербезпеки та безпеки інфраструктури (CISA), Національного інституту стандартів та технологій (NIST), Організації Північноатлантичного договору (NATO), а також визнаних зазначеними організаціями процедур оцінки відповідності, у тому числі сертифікації, рекомендованої для застосування у сферах організації спеціального зв'язку, криптографічного та технічного захисту інформації, кіберзахисту;";

6) підпункти 77 та 81 викласти в такій редакції:

"77) установлює порядок організації та забезпечення служби з охорони об'єктів, приміщень, систем, мереж урядового і спеціального зв'язку, ключових документів та державних шифрів до засобів криптографічного захисту інформації; ";

"81) організовує відповідно до законодавства підготовку, перепідготовку та підвищення кваліфікації осіб у сферах криптографічного та технічного захисту інформації, кіберзахисту, електронних комунікацій та радіочастотного спектра;";

7) в абзаці третьому підпункту 87 слова “, засобів, комплексів та систем спеціального зв’язку” виключити;

8) підпункти 95^5 і 95^6 викласти в такій редакції:

“95^5) забезпечує методичне регулювання оцінювання стану кіберзахисту, стану захищеності інформації, проведення оцінювання стану кіберзахисту інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси, службова інформація та інформація, що становить державну таємницю, стану кіберзахисту об’єктів критичної інформаційної інфраструктури та об’єктів критичної інфраструктури;

95^6) встановлює вимоги до суб’єктів оцінювання стану кіберзахисту щодо оцінювання інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інформаційної інфраструктури;”;

9) у підпункті 95^7 слова “урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA” замінити словами “національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA (національний CSIRT)”;

10) доповнити пункт підпунктами 95^{25}—95^{46} такого змісту:

“95^{25}) встановлює вимоги щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов’язаного з постачанням товарів, робіт і послуг власникам або розпорядникам інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інформаційної інфраструктури. З метою встановлення зазначених вимог Адміністрація Держспецзв’язку:

визначає критерії критичності таких товарів, робіт, послуг;

встановлює порядок визначення власниками або розпорядниками інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інформаційної інфраструктури рівня ризику, пов’язаного з критичністю таких товарів, робіт, послуг для забезпечення функціонування та заходів безпеки, що відповідають такому ризику;

встановлює порядок підтвердження постачальниками товарів, робіт, послуг відповідності впроваджених заходів безпеки інформації встановленим вимогам відповідно до рівня ризику, пов’язаного з постачанням товарів, робіт, послуг;

95^{26}) забезпечує реалізацію та дотримання порядку пошуку та/або виявлення потенційних вразливостей в інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або

інформація з обмеженим доступом, та на об’єктах критичної інформаційної інфраструктури;

95[27]) забезпечує організацію та систематичне проведення консультацій (навчань) з питань захисту інформації та кіберзахисту та оцінювання стану кіберзахисту для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи із захисту інформації або кіберзахисту в органах державної влади, інших державних органах, органах місцевого самоврядування, що є власниками або розпорядниками інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, та в юридичних особах, які є власниками або розпорядниками об’єктів критичної інформаційної інфраструктури;

95[28]) розробляє та забезпечує оновлення методичних рекомендацій щодо проведення інструктажів та тренінгів щодо кібергігієни на період призначення на посади державних службовців, працівників органів державної влади та інших державних органів, військовослужбовців, керівників та працівників державних підприємств, установ та організацій;

95[29]) надає з урахуванням професійних стандартів методичні рекомендації щодо типових вимог до підрозділів із кіберзахисту, загальних вимог до керівників із кіберзахисту в органах державної влади, інших державних органах, державних установах, організаціях, а також до осіб, які виконують функції та завдання керівників із кіберзахисту в юридичних особах щодо об’єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких вони є, та в органах місцевого самоврядування;

95[30]) забезпечує нормативно-правове регулювання відносин у сферах стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;

95[31]) забезпечує розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення та запровадження стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам у порядку, встановленому Кабінетом Міністрів України;

95[32]) призначає орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам із числа установ і організацій Держспецзв’язку;

95[33]) забезпечує реалізацію та методичне керівництво авторизацією з безпеки, порядок проведення якої затверджується Кабінетом Міністрів України;

95[34]) затверджує порядок ведення переліку авторизованих систем з безпеки, включення таких систем до переліку та виключення з нього, надання доступу до зазначеного переліку та інформації з нього;

95[35]) запроваджує та забезпечує функціонування системи професійної кваліфікації за групами кваліфікації у сферах захисту інформації та кіберзахисту, системи оцінювання та визнання таких кваліфікацій на основі відповідних професійних стандартів, затвердження в установленому порядку відповідних професійних стандартів, дотримання яких є обов'язковим в органах державної влади, інших державних органах, органах місцевого самоврядування, державних установах, організаціях та які рекомендуються до застосування на об'єктах критичної інфраструктури;

95[36]) створює та забезпечує функціонування кваліфікаційного центру за групами кваліфікацій у сферах безпеки інформації та кіберзахисту;

95[37]) забезпечує функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;

95[38]) координує діяльність об'єктів критичної інфраструктури з питань кіберзахисту у разі введення надзвичайного або воєнного стану;

95[39]) забезпечує функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

95[40]) забезпечує функціонування регіональних центрів кіберзахисту;

95[41]) визначає завдання із забезпечення функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози:

основні завдання, що можуть бути делеговані національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA галузевим та регіональним командам реагування на кіберінциденти, кібератаки, кіберзагрози, та порядок взаємодії команд реагування з CERT-UA;

вимоги до організаційно-технічної спроможності, сервісу, пов'язаного з реагуванням на кіберінциденти національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози, а також інших команд реагування в частині виконання ними завдань галузевої або регіональної команди реагування або в частині надання ними сервісу, пов'язаного з реагуванням на кіберінциденти, органам державної влади, іншим державним органам, органам місцевого самоврядування, операторам критичної інфраструктури, власникам або розпорядникам об'єктів критичної інформаційної інфраструктури;

порядок ведення репозитарію інформації про кіберінциденти, таксономій кіберінцидентів та їх версій;

порядок здійснення моніторингу за діяльністю національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози, а також інших команд реагування в частині виконання ними завдань галузевої або регіональної команди реагування або

в частині надання ними сервісу, пов’язаного з реагуванням на кіберінциденти, органам державної влади, іншим державним органам, органам місцевого самоврядування, операторам критичної інфраструктури, власникам або розпорядникам об’єктів критичної інформаційної інфраструктури, зокрема щодо додержання вимог закону в частині функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози відповідно до сфери їх повноважень та надання вимог про усунення порушень;

порядок здійснення заходів реагування у кризовій ситуації в кіберпросторі;

підстави для надання на основі отриманої від національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA інформації вимог про реагування власникам або розпорядникам інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інформаційної інфраструктури, операторам критичної інфраструктури, а також визначення строків та порядку реалізації визначених відповідною вимогою про реагування заходів реагування та подання звіту про їх виконання;

95[42]) визначає завдання із забезпечення функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози:

порядок обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, форми повідомлення, національної таксономії кіберінцидентів;

критерії визначення значного кіберінциденту, в тому числі для цілей виконання зобов’язань, визначених законодавством про здійснення повідомлень про кіберінциденти;

95[43]) запроваджує організаційно-технічні заходи щодо створення національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

95[44]) забезпечує функціонування платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та встановлення порядку приєднання до такої платформи;

95[45]) затверджує порядок атестації комплексу технічного захисту інформації для обробки інформації, що становить державну таємницю;

95[46]) забезпечує формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання;”.

3. Пункт 6 доповнити підпунктами 13 і 14 такого змісту:

“13) надавати обов’язкові до виконання вимоги про усунення встановлених відповідно до закону порушень законодавства щодо функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, щодо виконання вимог законодавства за результатами моніторингу в порядку, визначеному законодавством щодо діяльності команд реагування на кіберінциденти, кібератаки, кіберзагрози;

14) у визначених законодавством випадках вживати заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози шляхом надання обов’язкових до виконання вимог про реагування власникам або розпорядникам інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, та власникам або розпорядникам об’єктів критичної інформаційної інфраструктури.”.

_____