Додаток до вих. ІнАУ від 10.08.2023 № 74

Зауваження та пропозиції ІнАУ до проекту Наказу Адміністрації Держспецзв'язку «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)»

Положення у редакції проекту Вимог	**Положення до проекту Вимоги, запропоновані ІнАУ**	**Обґрунтування, пояснення**
I. Загальні положення .. 2. У цих Вимогах терміни вживаються в такому значенні: аудитор інформаційної безпеки на об'єктах критичної інфраструктури (далі – аудитор) – це аудитор інформаційної безпеки, що пройшов атестацію відповідно до встановленого порядку та включений до Переліку аудиторів інформаційної безпеки на об'єктах критичної інфраструктури (далі – Перелік); аудитор систем менеджменту інформаційної безпеки на об'єктах критичної інфраструктури (далі – аудитор систем менеджменту) – фізична особа, яка має право проводити незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури самостійно та у складі команди з аудиту інформаційної безпеки на об'єктах критичної інфраструктури та дані про яку внесені до Переліку; … команда з аудиту інформаційної безпеки на об'єктах критичної інфраструктури (далі –	I. Загальні положення … 2. У цих Вимогах терміни вживаються в такому значенні: аудитор інформаційної безпеки на об'єктах критичної інфраструктури (далі – аудитор) – це аудитор інформаційної безпеки, що пройшов атестацію відповідно до встановленого порядку, **має право проводити незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури самостійно та у складі команди з аудиту інформаційної безпеки** та включений до Переліку аудиторів інформаційної безпеки на об'єктах критичної інфраструктури (далі – Перелік); **Виключити** **…** команда з аудиту інформаційної безпеки на об'єктах критичної інфраструктури (далі –	В ЗУ "Про основні засади забезпечення кібербезпеки України" та в постанові КМУ від 24 березня 2023 року № 257 "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури" вказано лише про аудиторів інформаційної безпеки та порядок їх атестації (переатестації). Вищі законодавчі акти (в порівняння з наказом Держспецзв'язку) не зазначають про доцільність створення «аудиторів систем менеджменту інформаційної безпеки». Крім того, відповідно до повноважень, закріплених у п. 90 ч. ст. 14 ЗУ "Про Державну службу спеціального зв'язку та захисту інформації України", на Держспецзв'язку відповідно до визначених завдань покладаються обов'язки, зокрема, забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації). З урахуванням зазначеного пропонується доповнення до визначення поняття «аудитор інформаційної безпеки на об'єктах критичної інфраструктури» та його викладення у новій редакції, а також уточнення до поняття

команда з аудиту) – група осіб, яка складається з керівника команди з аудиту та залучених до неї аудиторів систем менеджменту та/або провідних аудиторів ІТ;	команда з аудиту) – група осіб, яка складається з керівника команди з аудиту та залучених до неї **аудиторів інформаційної безпеки** та/або провідних аудиторів ІТ;	«команда з аудиту інформаційної безпеки на об'єктах критичної інфраструктури».
ІІ. Вимоги до заявників … 2. Підтвердженням досвіду роботи у сфері інформаційної безпеки та/або інформаційних систем є: відомості про виконання не менше ніж 4 проєктів з внутрішнього або незалежного аудиту інформаційної безпеки за останні 2 роки ~~або~~ ~~відомості про обіймання посад та/або виконання робіт за дорученням на умовах угод (договорів, контрактів), що безпосередньо пов'язані із забезпеченням захисту інформації та кібербезпеки, упродовж останніх 2 років в органах державної влади, на підприємствах, в установах, організаціях незалежно від форми власності.~~	ІІ. Вимоги до заявників … 2. Підтвердженням досвіду роботи у сфері інформаційної безпеки та/або інформаційних систем є: відомості про виконання не менше ніж 4 проєктів з внутрішнього або незалежного аудиту інформаційної безпеки за останні 2 роки. **Виключити**	Пропонується дане положення або виключити або суттєво доопрацювати, оскільки запропонований критерій підтвердження досвіду роботи у сфері інформаційної безпеки та/або інформаційних систем є досить сумнівним. Зокрема, не вказано, 1) які саме відомості можуть бути таким підтвердженням, тобто, це записи у трудовій книжці тощо, 2) які функції заявник повинен виконувати, щоб запевнити достатність своєї кваліфікації тощо. Якщо це записи у трудовій книжці, то потрібно зазначити переліки (чи коди) посад, які можуть вважатись підтвердження досвіду роботи у сфері інформаційної безпеки.
ІІІ. Порядок атестації (переатестації) заявників 1. Для включення до Переліку заявник, який є фізичною особою, надсилає такі документи: … 2) документи, що підтверджують відповідність заявника вимогам, визначеним у пункті 1 розділу ІІ цих Вимог, а саме: … копію трудової книжки та/або 4 ~~рекомендаційних листи-відгуків або~~ контрактів на проведення робіт з аудиту	ІІІ. Порядок атестації (переатестації) заявників 1. Для включення до Переліку заявник, який є фізичною особою, надсилає такі документи: … 2) документи, що підтверджують відповідність заявника вимогам, визначеним у пункті 1 розділу ІІ цих Вимог, а саме: … копію трудової книжки та/або 4 контрактів на проведення робіт з аудиту інформаційної	Підтвердження рекомендаційними листами-відгуками кваліфікації та обсягу практичного застосування знань у сфері інформаційної безпеки є сумнівним.

інформаційної безпеки, що були проведені протягом двох календарних років до дати подання заяви; … копію трудового договору з юридичною особою з терміном не менше 1 року; копію сертифікату «Аудитор систем менеджменту інформаційної безпеки на об'єктах критичної інфраструктури», «Керівник команди з аудиту інформаційної безпеки» або «Провідний аудитор інформаційних технологій (з кібербезпеки)» відповідно до вимог професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)» виданого Кваліфікаційним центром або Органом з сертифікації персоналу. **Відсутній** 2. Для включення до Переліку заявник, який є юридичною особою, надсилає такі документи: … інформацію (довідку у довільній формі) про те, що до заявника не застосовані санкції на підставі нормативно-правових актів, прийнятих згідно із Законом України «Про санкції»; копії свідоцтва про включення до Реєстру аудиторських фірм та аудиторів або атестату про акредитацію, виданого Національним	безпеки, що були проведені протягом двох календарних років до дати подання заяви; … копію трудового договору з юридичною особою з терміном не менше 1 року; копію сертифікату «Аудитор систем менеджменту інформаційної безпеки на об'єктах критичної інфраструктури», «Керівник команди з аудиту інформаційної безпеки» або «Провідний аудитор інформаційних технологій (з кібербезпеки)» відповідно до вимог професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)» виданого Кваліфікаційним центром або Органом з сертифікації персоналу. **Включення заявника до Переліку здійснюється після його перевірки в межах своїх повноважень Службою безпеки України.** 2. Для включення до Переліку заявник, який є юридичною особою, надсилає такі документи: … інформацію (довідку у довільній формі) про те, що до заявника не застосовані санкції на підставі нормативно-правових актів, прийнятих згідно із Законом України «Про санкції»; копії свідоцтва про включення до Реєстру аудиторських фірм та аудиторів або атестату	Дане доповнення пропонується з метою перевірки та недопущення допуску до інформації на об'єктах критичної інфраструктури осіб, які, скомпрометовані та мали/мають зв'язок з ворожими країнами.

агентством з акредитації відповідно до ДСТУ EN ISO/IEC 17021-1:2017 та ДСТУ EN ISO/IEC 27006, та свідоцтва про відповідність системи контролю якості. **Відсутній**	про акредитацію, виданого Національним агентством з акредитації відповідно до ДСТУ EN ISO/IEC 17021-1:2017 та ДСТУ EN ISO/IEC 27006, та свідоцтва про відповідність системи контролю якості. **Включення заявника до Переліку здійснюється після перевірки працівників заявника в межах своїх повноважень Службою безпеки України.**	Пояснення див. вище.
V. Виключення аудиторів з Переліку та їх переатестація 1. Рішення про виключення фізичної особи з Переліку приймається у разі: … порушення аудитором законодавства у сфері захисту інформації; … 2. Рішення про виключення юридичної особи з Переліку приймається у разі: порушення юридичною особою вимог законодавства у сфері захисту інформації; …	V. Виключення аудиторів з Переліку та їх переатестація 1. Рішення про виключення фізичної особи з Переліку приймається у разі: … порушення аудитором законодавства у сфері захисту інформації, **що підтверджено рішенням суду або рішенням органу державної влади**; … 2. Рішення про виключення юридичної особи з Переліку приймається у разі: порушення юридичною особою вимог законодавства у сфері захисту інформації, **що підтверджено рішенням суду або рішенням органу державної влади**; …	Пропонуються уточнення, що порушення повинні бути підтверджені відповідними рішеннями.