Прим. № ___

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

Департамент державного контролю у сфері захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України (ДДК Адміністрації Держспецзв'язку)

вул. Солом'янська, 13, м. Київ, Україна, 03110,
тел./факс: (044) 281-88-50
e-mail: ddk@cip.gov.ua

_____ № _____

Інтернет Асоціація України

За результатами громадського обговорення та зовнішнього погодження, Департаментом доопрацьовано проєкт наказу Адміністрації Держспецзв'язку «Про затвердження Вимог до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядку їх атестації (переатестації)» (далі – проєкт Наказу).

Пропозиції, надані листом від 10.08.2023 № 74, були враховані в повній мірі.

Додатки: 1. Проєкт наказу на 11 арк.
2. Порівняльна таблиця до проєкту наказу на 6 арк.

З повагою

Директор Департаменту Олег БОНДАРЕНКО

Артем Скопич 066 922 2545

ПРОЄКТ
Прим. №__

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УРАЇНИ

Н А К А З

м. Київ

__ _____ 20__ року № _____

Про затвердження Вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації)

Відповідно до пункту 90 частини першої статті 14 Закону України “Про Державну службу спеціального зв’язку та захисту інформації України”, пункту 1 частини другої статті 8 Закону України “Про основні засади забезпечення кібербезпеки України”, підпункту 95^5 пункту 4, пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, пункту 2 постанови Кабінету Міністрів України від 24 березня 2023 року № 257 “Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури”, з метою врегулювання питань забезпечення впровадження системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки та порядку їх атестації (переатестації)

НАКАЗУЮ:

1. Затвердити Вимоги до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядок їх атестації (переатестації), що додаються.

2. Директору Департаменту державного контролю у сфері захисту інформації Адміністрації Державної служби спеціального зв’язку та захисту інформації України забезпечити подання цього наказу в установленому порядку на державну реєстрацію до Міністерства юстиції України.

3. Контроль за виконанням цього наказу покласти на заступника Голови Державної служби спеціального зв’язку та захисту інформації України відповідно до розподілу обов’язків.

4. Цей наказ набирає чинності з дня його офіційного опублікування.

Голова Служби
бригадний генерал Юрій ЩИГОЛЬ

ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної
служби спеціального зв’язку та
захисту інформації України
___ _____ 20__ року № ___

Вимоги
до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядок їх атестації (переатестації)

I. Загальні положення

1. Ці Вимоги встановлюють критерії та вимоги до осіб, які планують отримати право проводити незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури, а також визначають порядок їх атестації (переатестації), включення до Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та виключення з нього.

2. У цих Вимогах терміни вживаються в такому значенні:

Перелік аудиторів інформаційної безпеки на об’єктах критичної інфраструктури (далі – Перелік) – список атестованих аудиторів інформаційної безпеки, який містить дані про прізвище, власне ім’я, по батькові (за наявності)/назву аудитора інформаційної безпеки, кваліфікацію (для фізичних осіб-аудиторів), контактні дані, кількість проведених аудитів, рейтинг аудитора інформаційної безпеки за результатами проведених аудитів і розміщується на сайті Держспецзв’язку в розділі «Незалежний аудит інформаційної безпеки»;

заявник – юридична або фізична особа, що має намір провадити діяльність аудитора інформаційної безпеки на об’єктах критичної інфраструктури, пройти атестацію (переатестацію) аудиторів інформаційної безпеки та бути включеною до Переліку;

атестація аудиторів інформаційної безпеки (далі – атестація) – процедура розгляду та перевірки на відповідність цим Вимогам документів заявників з метою отримання ними права проводити незалежні аудити інформаційної безпеки на об’єктах критичної інфраструктури;

Кваліфікаційний центр – суб’єкт, уповноважений Національним агентством кваліфікацій здійснювати оцінювання і визнання результатів навчання, здобутих особами шляхом формальної, неформальної або інформальної освіти, присвоєння та/або підтвердження відповідних професійних кваліфікацій, визнання відповідних професійних кваліфікацій,

здобутих у інших країнах, на підставі сертифіката про акредитування такого кваліфікаційного центру і включений до Реєстру кваліфікаційних центрів у складі Реєстру кваліфікацій;

Орган із сертифікації персоналу – суб'єкт, який має атестат про акредитацію, виданий Національним агентством з акредитації України, та надає послуги із сертифікації персоналу згідно з вимогами кваліфікацій «Провідний аудитор систем менеджменту інформаційної безпеки на об'єктах критичної інфраструктури», «Керівник команди з аудиту інформаційної безпеки» та «Провідний аудитор інформаційних технологій (з кібербезпеки)», визначених у професійному стандарті «Аудитор інформаційних технологій (з кіберебезпеки)».

Інші терміни вживаються у значенні, наведеному в Законах України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, затвердженому постановою Кабінету Міністрів України від 24 березня 2023 року № 257.

3. Суб'єктами відносин, пов'язаних з атестацією (переатестацією) аудиторів інформаційної безпеки, є:

Адміністрація Держспецзв'язку;

заявники;

Кваліфікаційні центри;

Органи із сертифікації персоналу;

Служба безпеки України.

4. Адміністрація Держспецзв'язку:

здійснює ведення та оприлюднення Переліку на сайті Держспецзв'язку в розділі «Незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури»;

отримує, розглядає та перевіряє документи, подані заявниками;

приймає рішення про успішне проходження атестації та включення заявника до Переліку або про не проходження атестації заявником;

приймає рішення про скасування права на проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та виключення аудитора інформаційної безпеки з Переліку.

5. Підтвердженням проходження заявником атестації є відповідне рішення Адміністрації Держспецзв'язку та наявність відомостей про нього в Переліку.

6. Рішення Адміністрації Держспецзв'язку та наявність відомостей про юридичну особу в Переліку підтверджує право юридичної особи проводити

незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури, залучаючи до нього виключно аудиторів інформаційної безпеки, які пройшли атестацію в порядку, що встановлений цими Вимогами, і з якими вона має договірні відносини.

ІІ. Вимоги до заявників

1. Вимоги до заявника, який є фізичною особою:

бути громадянином України;

не мати не погашеної або не знятої судимості в установленому законом порядку;

мати довідку встановленого законодавством зразка про відсутність психіатричних протипоказань;

мати допуск до державної таємниці;

мати документи, що підтверджують досвід роботи у сфері інформаційної безпеки та/або інформаційних систем;

мати чинний сертифікат «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки» відповідно до вимог професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)», виданий Кваліфікаційним центром або Органом із сертифікації персоналу.

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.

3. Вимоги до заявника, який є юридичною особою:

перебувати у трудових відносинах не менше ніж з 3 аудиторами інформаційної безпеки, які пройшли атестацію згідно з цими Вимогами та включені до Переліку;

мати дозвіл на провадження діяльності, пов’язаної з державною таємницею;

не бути включеним до переліку осіб, щодо яких застосовано спеціальні економічні та інші обмежувальні заходи (санкції) відповідно до Закону України «Про санкції»;

мати атестат про акредитацію, виданий Національним агентством з акредитації відповідно до ДСТУ EN ISO/IEC 17021-1:2017 та ДСТУ EN ISO/IEC 27006.

ІІІ. Порядок атестації (переатестації) заявників

1. З метою проходження атестації (переатестації) та включення до Переліку заявник, який є фізичною особою, надсилає до Адміністрації Держспецзв’язку такі документи:

1) заповнену заяву за формою згідно з додатком 1 до цих Вимог;

2) документи, що підтверджують відповідність заявника вимогам, визначеним у пункті 1 розділу ІІ цих Вимог, а саме:

копію витягу про відсутність судимості або обмежень;

довідку встановленого законодавством зразка про проходження психіатричних оглядів, у тому числі на предмет вживання психоактивних речовин;

копії 4 контрактів на проведення робіт з аудиту інформаційної безпеки, що були проведені протягом двох календарних років до дати подання заяви;

копію допуску до державної таємниці;

копію сертифіката «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки» відповідно до вимог професійного стандарту «Аудитор інформаційних технологій (з кібербезпеки)», виданого Кваліфікаційним центром або Органом із сертифікації персоналу.

2. З метою проходження атестації (переатестації) та включення до Переліку заявник, який є юридичною особою, надсилає такі документи:

1) заповнену заяву за формою згідно з додатком 2 до цих Вимог;

2) документи, що підтверджують відповідність заявника вимогам, визначеним у пункті 3 розділу ІІ цих Вимог, а саме:

копії чинних сертифікатів «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки» та трудових договорів заявника з аудиторами, яким належать ці сертифікати;

копію дозволу на провадження діяльності, пов’язаної з державною таємницею;

інформацію (довідку у довільній формі) про те, що до заявника не застосовані спеціальні економічні та інші обмежувальні заходи (санкції) відповідно до Закону України «Про санкції»;

копію атестата про акредитацію, виданого Національним агентством з акредитації відповідно до ДСТУ EN ISO/IEC 17021-1:2017 та ДСТУ EN ISO/IEC 27006.

3. Заява з відповідними документами подаються заявником до Адміністрації Держспецзв’язку в паперовій або електронній формі. Електронна пошта для надсилання документів заявником вказана на сайті Держспецзв’язку в розділі «Незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури».

4. Документи, які надаються заявником на розгляд, повинні відповідати таким вимогам:

заява має бути викладена державною мовою;

документи, викладені іноземною мовою, повинні бути перекладені на державну мову із засвідченням правильності перекладу з однієї мови на іншу в установленому законодавством порядку;

заява та документи повинні містити повну та достовірну інформацію, передбачену цими Вимогами.

5. Адміністрація Держспецзв'язку погоджує зі Службою безпеки України у межах компетенції атестацію (переатестацію) заявника шляхом надання до Служби безпеки України копій документів, передбачених пунктами 1 та 2 розділу III цих Вимог, для перевірки заявника на предмет його сприяння діяльності іноземної держави, іноземної організації чи їх представників, що може завдати шкоди інтересам національної безпеки України, або інші його дії, які створюють реальні та/або потенційні загрози національним інтересам та безпеці.

Про прийняте рішення Служба безпеки України повідомляє Адміністрацію Держспецзв'язку протягом десяти робочих днів з дня отримання відповідного листа.

6. Підставами для прийняття рішення щодо не проходження атестації заявником є:

подання документів або відомостей, визначених цими Вимогами, не в повному обсязі;

невідповідність документів вимогам, які встановлені цими Вимогами;

невідповідність заявника зазначеним вище вимогам;

не підтверджена (не може бути підтверджена) достовірність наданих документів;

отримання від Служби безпеки України повідомлення про прийняте рішення щодо не погодження атестації заявника.

IV. Прийняття рішення про успішне проходження атестації заявника та включення його до Переліку

1. У разі відповідності поданої заяви та документів вимогам, що встановлені цими Вимогами, та з урахуванням повідомлення Служби безпеки України щодо погодження атестації (переатестації) заявника Адміністрація Держспецзв'язку протягом 15 робочих днів з моменту отримання заяви приймає рішення про успішне проходження атестації та включення заявника до Переліку та вносить відповідні зміни до Переліку на основі цього рішення протягом 5 робочих днів з моменту прийняття рішення.

Повідомлення заявника про успішне проходження атестації та включення його до Переліку відбувається протягом 5 робочих днів з моменту прийняття рішення шляхом надсилання листа на електронну пошту заявника.

2. У випадку прийняття рішення щодо не проходження атестації заявником Адміністрація Держспецзв'язку протягом 5 робочих днів з моменту прийняття

такого рішення повідомляє йому причини, з яких йому було відмовлено, шляхом надсилання листа на його електронну пошту.

Після усунення причин, що були підставою для прийняття рішення щодо не проходження атестації заявником, він може повторно подати документи до Адміністрації Держспецзв'язку відповідно до порядку атестації, що встановлений цими Вимогами.

3. Після успішного проходження атестації та включення фізичної особи до Переліку вона зобов'язана щороку до 1 лютого надсилати до Адміністрації Держспецзв'язку інформацію про чинний допуск до державної таємниці, чинний сертифікат «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки» або «Керівник команди з аудиту систем менеджменту інформаційної безпеки».

4. Після успішного проходження атестації та включення юридичної особи до Переліку вона зобов'язана щороку до 1 березня надсилати до Адміністрації Держспецзв'язку інформацію про чинний дозвіл на провадження діяльності, пов'язаної з державною таємницею, чинні сертифікати аудиторів інформаційної безпеки та трудові договори з аудиторами, яким належать ці сертифікати.

5. У разі зміни інформації, що міститься в документах, які аудитор інформаційної безпеки подав до Адміністрації Держспецзв'язку для проходження атестації відповідно до пунктів 1 та 2 розділу III цих Вимог, він зобов'язаний надати інформацію про зміни до Адміністрації Держспецзв'язку впродовж 30 календарних днів з моменту виникнення такої зміни.

V. Виключення аудиторів інформаційної безпеки з Переліку та їх переатестація

1. Рішення про скасування права на проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та виключення фізичної особи з Переліку приймається у разі:

ведення кримінального провадження та в разі висунення обвинувального вироку за вчинення умисного кримінального правопорушення. Дані про фізичну особу в Переліку відновлюються у разі закриття кримінального провадження з виправдовувальним вироком або без оголошення вироку;

порушення аудитором інформаційної безпеки законодавства у сфері захисту інформації та кібербезпеки, що підтверджено рішенням суду або рішенням органу державної влади;

зміни особистої інформації, інформації щодо чинного сертифіката «Провідний аудитор інформаційних технологій (з кібербезпеки)», «Провідний аудитор систем менеджменту інформаційної безпеки», «Керівник команди з аудиту систем менеджменту інформаційної безпеки», що призвели до невиконання вимог, визначених пунктом 1 розділу II цих Вимог;

позбавлення допуску до державної таємниці;

отримання від Служби безпеки України повідомлення з аргументованою пропозицією щодо виключення аудитора інформаційної безпеки з Переліку у зв'язку зі його сприянням діяльності іноземної держави, іноземної організації чи їх представників, що може завдати шкоди інтересам національної безпеки України, або іншими діями аудитора інформаційної безпеки, які створюють реальні та/або потенційні загрози національним інтересам та безпеці;

отримання заяви у довільній формі від аудитора інформаційної безпеки про припинення діяльності аудитора інформаційної безпеки на об'єктах критичної інфраструктури за власним бажанням.

2. Рішення про скасування права на проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та виключення юридичної особи з Переліку приймається у разі:

порушення юридичною особою вимог законодавства у сфері захисту інформації та кібербезпеки, що підтверджено рішенням суду або рішенням органу державної влади;

зміни інформації щодо трудових відносин з аудиторами інформаційної безпеки, що призвели до невиконання юридичною особою вимог до заявників, визначених пунктом 3 розділу II цих Вимог;

скасування або закінчення дії атестата про акредитацію, виданого Національним агентством з акредитації відповідно до ДСТУ EN ISO/IEC 17021-1:2017 та ДСТУ EN ISO/IEC 27006;

скасування або закінчення дії дозволу на провадження діяльності, пов'язаної з державною таємницею;

отримання від Служби безпеки України повідомлення з аргументованою пропозицією щодо виключення аудитора інформаційної безпеки з Переліку у зв'язку зі його сприянням діяльності іноземної держави, організації чи їх представникам, що може завдати шкоди інтересам національної безпеки України, або іншими діями аудитора інформаційної безпеки, які створюють реальні та/або потенційні загрози національним інтересам та безпеці;

отримання заяви у довільній формі від аудитора інформаційної безпеки про припинення діяльності аудитора інформаційної безпеки на об'єктах критичної інфраструктури за власним бажанням.

3. У разі виключення аудитора інформаційної безпеки з Переліку для проходження переатестації, поновлення права на проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та включення його до Переліку він повинен подати до Адміністрації Держспецзв'язку документи відповідно до положень розділу III цих Вимог.

Директор Департаменту державного
контролю у сфері захисту інформації
Адміністрації Держспецзв'язку Олег БОНДАРЕНКО

Додаток 1
до Вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації)
(пункт 1 розділу III)

Заява
про проходження атестації та включення до Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури (для фізичних осіб)

1. Заявник _____
(прізвище, власне ім'я, по батькові (у разі наявності))

2. Дата народження _____

3. Реквізити документа, що підтверджує особу _____

_____
(найменування документа, серія, номер, ким виданий і коли)

4. Ідентифікаційний код _____

5. Адреса для листування _____

_____
(поштовий індекс, область/Автономна Республіка Крим, район, населений пункт, вулиця/провулок, площа тощо, № будинку/корпусу, № квартири/офісу)

6. Контактний телефон _____, електронна пошта _____

7. До заяви додаю:

_____
(повний перелік документів, що додаються до заяви, із зазначенням для кожного: копія чи оригінал, найменування, номер, дата видачі документа)

_____
_____
_____
_____
_____

_____ _____
(дата) *(підпис)*

* Примітка. Документи, що додаються до заяви, визначені у Вимогах до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації).

Додаток 2
до Вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації) (пункт 2 розділу III)

Заява
про проходження атестації та включення до Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури (для юридичних осіб)

1. Заявник _____
(повне найменування юридичної особи)

_____
(код платника податків згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб - підприємців та громадських формувань або податковий номер)

_____
(код Класифікації видів економічної діяльності (КВЕД))

має намір провадити діяльність у сфері аудиту інформаційної безпеки на об’єктах критичної інфраструктури і просить включити його до Переліку аудиторів інформаційної безпеки на об’єктах критичної інфраструктури.

2. Місцезнаходження заявника _____

_____

3. Адреса для листування _____

_____
(поштовий індекс, область/Автономна Республіка Крим, район, населений пункт, вулиця/провулок, площа тощо, № будинку/корпусу, № квартири/офісу)

4. Контактний телефон _____, електронна пошта _____

5. Адреса вебсайту у мережі Інтернет (URL) _____

6. Прізвище, власне ім'я, по батькові (у разі наявності) керівника _____

7. Номер і дата видачі атестата про акредитацію, виданого Національним агентством з акредитації

_____

Керівник _____ _____
(підпис) (власне ім’я, прізвище)

«___» _____ 20__ року

М.П.

_____

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**	**Внесені зміни або аргументи щодо відхилення зауважень**
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	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**	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	**Враховано** Дані положенні вилучені з проєкту наказу

інфраструктури та дані про яку внесені до Переліку; … команда з аудиту інформаційної безпеки на об'єктах критичної інфраструктури (далі – 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 інформаційної безпеки на об'єктах критичної інфраструктури (далі – команда з аудиту) – група осіб, яка складається з керівника команди з аудиту та залучених до неї **аудиторів інформаційної безпеки** та/або провідних аудиторів ІТ;	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 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.	**Враховано в запропонованій редакції**

III. 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 II цих Вимог, а саме: … копію трудової книжки та/або 4 ~~рекомендаційних листи відгуків або~~ контрактів на проведення робіт з аудиту 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	III. 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 II цих Вимог, а саме: … копію трудової книжки та/або 4 контрактів на проведення робіт з аудиту 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)»	Підтвердження рекомендаційними листами-відгуками кваліфікації та обсягу практичного застосування знань у сфері інформаційної безпеки є сумнівним. Дане доповнення пропонується з метою перевірки та недопущення допуску до інформації на об'єктах критичної інфраструктури осіб, які,	**Враховано в запропонованій редакції**

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 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**	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 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.**	скомпрометовані та мали/мають зв’язок з ворожими країнами. Пояснення див. вище.	**Враховано** Розділ ІІІ доповнено новим пунктом: «5. Адміністрація Держспецзв’язку погоджує зі Службою безпеки України у межах компетенції атестацію (переатестацію) заявника шляхом надання до Служби безпеки України копій документів, передбачених пунктами 1 та 2 розділу ІІІ цих Вимог, для перевірки заявника на предмет його сприяння діяльності іноземної держави, іноземної організації чи їх представників, що може завдати шкоди інтересам національної безпеки України, або інші його дії, які створюють реальні та/або потенційні загрози національним інтересам та безпеці. Про прийняте рішення Служба безпеки України повідомляє Адміністрацію Держспецзв’язку протягом десяти робочих днів з дня отримання відповідного листа.»

			Пункт 5 розділу ІІІ змінено на пункт 6 та доповнено наступним положенням: «6. Підставами для прийняття рішення щодо не проходження атестації заявником є: … отримання від Служби безпеки України повідомлення про прийняте рішення щодо не погодження атестації заявника.» Також доповнено пункт 1 та 2 Розділу V наступним положенням: «отримання від Служби безпеки України повідомлення з аргументованою пропозицією щодо виключення аудитора інформаційної безпеки з Переліку у зв’язку зі його сприянням діяльності іноземної держави, іноземної організації чи їх представників, що може завдати шкоди інтересам національної безпеки України, або іншими діями аудитора інформаційної безпеки, які створюють

			реальні та/або потенційні загрози національним інтересам та безпеці;»
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.	**Враховано в запропонованій редакції**