

Додаток 64. КРИТЕРІЇ ОЦІНЮВАННЯ КОМПЕТЕНТНОСТІ ФАХІВЦІВ ЗА КВАЛІФІКАЦІЄЮ «ВНУТРІШНІЙ АУДИТОР СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ» [ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT), ISO/IEC 27001:2013, ISO/IEC 27001:2022]Ф-55-81
Додаток 64 до ДП ОСП-18**Критерії оцінювання компетентності фахівців за кваліфікацією
«Внутрішній аудитор систем менеджменту інформаційної безпеки»
[ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT), ISO/IEC 27001:2013,
ISO/IEC 27001:2022]**

Внутрішній аудитор систем менеджменту інформаційної безпеки [ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT), ISO/IEC 27001:2013, ISO/IEC 27001:2022] кваліфікується в Органі сертифікації персоналу Української асоціації якості (ОСП УАЯ) для систематичного проведення внутрішніх аудитів систем менеджменту інформаційної безпеки відповідно до вимог міжнародних стандартів ДСТУ ISO/IEC 27001, ISO 19011 в діючій редакції, а також ведення робіт, пов'язаних із плануванням, перевіркою виконання та аналізом показників якості в процесі функціонування систем менеджменту інформаційної безпеки.

Вимоги до заявників на присвоєння кваліфікації «Внутрішній аудитор систем менеджменту інформаційної безпеки»

Теоретична підготовка для кваліфікації "внутрішній аудитор" повинна бути не менше **16 годин** і охоплювати такі питання:

- вимоги та настанови стандартів ДСТУ ISO/IEC 27001 і ISO 19011 в діючій редакції
- типи аудитів, внутрішні аудити систем менеджменту інформаційної безпеки;
- стандарти і настанови з систем менеджменту;
- основи внутрішніх аудитів;
- психологічні аспекти;
- планування та підготовка програм внутрішнього аудиту систем якості (керівництво програмою внутрішнього аудиту, роль і відповідальність внутрішнього аудитора, ведення записів, плани внутрішнього аудиту, підготовка та використання чек-листів, аналіз і моніторинг програми внутрішнього аудиту тощо);
- діяльність в процесі внутрішнього аудиту (аналіз документації, планування діяльності з внутрішнього аудиту, технології інтерв'ю, збір доказів, взаємодія з тими, хто підлягає внутрішньому аудиту, документування результатів перевірок і зауважень внутрішнього аудиту, визначення і класифікація невідповідностей, заключна нарада, коригувальні дії);
- звітність (підготовка і зміст звітів, затвердження, розповсюдження, зберігання звітів, конфіденційність);
- подальші дії (повторні внутрішні аудити, коригувальні дії).

Внутрішній аудитор повинен мати вищу освіту та виробничий досвід не менше 1-го року або освітньо-кваліфікаційний рівень молодшого спеціаліста та виробничий досвід не менше 2-х років в одному з таких видів діяльності як розробка, виробництво, технологія, будівництво, сфера послуг, управління, економіка.

Внутрішній аудитор повинен мати не менше 1 року практичного досвіду роботи, пов'язаного з відповідною системою менеджменту, або інтегрованими системами менеджменту. Діяльність розглядається як пов'язана з відповідною системою менеджменту, якщо вона була направлена на запровадження відповідних вимог і норм (наприклад, ДСТУ ISO/IEC 27001) з чітким визначенням особистої відповідальності.

Внутрішній аудитор повинен ознайомитися з Кодексом професійної поведінки і декларувати підписом, що він цілком і твердо буде дотримуватися його положень.

Внутрішній аудитор повинен бути компетентним спеціалістом, дипломатичним, здатним висловлювати авторитетну офіційну думку.

Внутрішній аудитор повинен мати аналітичні здібності, тверду волю, відчувати реальну ситуацію, розуміти складні процеси в широкій перспективі.

Внутрішній аудитор повинен бути чесним, кваліфікованим, готовим вчитися і вчити інших, відданим, мати здібність працювати в команді, бути здатним керувати.