АЛЬТЕРНАТИВА
центр сучасної сертифікації

ТОВ «ЦЕНТР СУЧАСНОЇ СЕРТИФІКАЦІЇ «АЛЬТЕРНАТИВА»
Юр. адреса: Україна, 02192, місто Київ, вулиця Малишка Андрія, будинок 1, приміщення 25-36. Адреса провадження діяльності: Україна, 03150, м. Київ, вул. Антоновича, буд. 48, офіс 6.
Код ЄДРПОУ: 44852948, ІПН 448529426534
alternatyva.com.ua alternatyva.cert@gmail.com +38(050)777-96-80

ВИТЯГ З ІНСТРУКЦІЇ ОС «ПОРЯДОК СЕРТИФІКАЦІЇ СИСТЕМ УПРАВЛІННЯ» (QI.09.01)

5 ПОРЯДОК ПРОВЕДЕННЯ СЕРТИФІКАЦІЇ СИСТЕМ УПРАВЛІННЯ

5.1 Подача заявки

Виробник продукції (процесів, послуг) (надалі продукції), який претендує на сертифікацію СУ, подає в ОС заявку (Ф-09.01-01) та опитувальну анкету (Ф-09.01-02). Організація будь-якої форми власності або будь-яка фізична особа має право провести в ОС сертифікацію системи управління. Організація-заявник може отримати інформацію стосовно порядку проведення сертифікації систем управління в ОС або з офіційного web-сайту alternatyva.com.ua.

5.2 Розгляд заявки

Визначений керівником ОС/заступником фахівець розглядає заявку та опитувальну анкету, реєструє заявку в «Журналі реєстрації заявок та видачі сертифікатів на системи управління», який ведеться в електронному вигляді, для проведення попереднього обстеження системи управління заявника та здійснює їх попередній розгляд на предмет визначення:

- бажаної сфери сертифікації;
- доречних деталей щодо організації-заявника, як вимагається конкретною схемою сертифікації, включаючи її назву і адресу(и) її ділянок(и), її процесів та діяльності, людських і технічних ресурсів, функцій і взаємозв'язків і будь-яких доречних юридичних зобов'язань;
- наявності інформації стосовно всіх процесів, які використовуються організацією на умовах аутсорсингу, які впливатимуть на відповідність вимогам;
- стандартів або інших вимог, на відповідність яким організація-заявник бажає отримати сертифікацію;
- наявності інформації щодо того, чи було проведено консультування з питань систем управління і, якщо так, то ким.

5.3 Перелік документації

Перелік документації, який надається підприємством до заявки, в залежності від сфери сертифікації, долучається до справи по сертифікації. Фахівець ОС, який проводив розгляд заявки, складає перелік документів, які додаються до заявки, відповідно до вимог застосовного стандарту, іншої додаткової документації з урахуванням специфіки підприємства-заявника та продукції, що ним виготовляється, вимог споживачів тощо.

5.4 Аналіз заявки

Аналіз заявки та наданої інформації до заявки проводиться, щоб упевнитись, що:

- інформація про організацію-заявника та її систему управління є достатньою для розробки програми аудиту;
- будь-які відомі непорозуміння між ОС та організацією-заявником вирішені;
- ОС має компетентність і спроможність виконувати сертифікаційну діяльність (Згідно наданих кодів КВЕД, враховуючи вимоги QI.07.01, відповідальний фахівець визначає до якої галузі економіки входить заявлена заявником сфера сертифікації та чи має в цій галузі технічну компетентність ОС);
- ОС здатний провести сертифікацію стосовно місцезнаходження виробничих ділянок організації-заявника, бажаної для заявника тривалості для проведення аудиту і

будь-які інші питання, що впливають на процес сертифікації, враховані (мова, умови безпеки, загрози неупередженості, тощо).

5.5 Результати розгляду

Результати розгляду заявки та вихідних документів, оформлюються протоколом (Ф-09.01-03) та рішенням (Ф-09.01-04). Примірники протоколу та рішення надаються заявнику.

Після розгляду заявки, ОС приймає або відхиляє заявку на сертифікацію.

Якщо ОС відхиляє заявку на сертифікацію, за результатами розгляду заявки, причини відхилення повинні бути документально оформлені і чітко доведені до замовника.

У разі позитивного рішення ОС та заявник укладають договір на сертифікацію СУ, який передбачає проведення робіт у два етапи:

1-ий етап аудиту - попереднє оцінювання СУ (попередня оцінка СУ);

2-ий етап аудиту - остаточна перевірка СУ (аудит на місці).

5.6 Підготовка до оцінювання

5.6.1 Базуючись на розгляді заявки та вихідних матеріалів відповідальна особа ОС визначає компетентність, необхідну для включення в групу аудиту і для прийняття рішення щодо сертифікації. Критерії компетентності персоналу регламентовані QI.07.01, QP.07.01.

Для проведення сертифікації СУЯ, СУПК керівник ОС/заступник призначає групу з аудиту для проведення робіт з сертифікації СУ.

Склад групи з аудиту та перелік осіб, які приймають рішення стосовно надання сертифікації зазначається в розпорядженні про призначення групи з аудиту для проведення сертифікації СУ (Ф-09.01-06).

До складу групи з аудиту має бути включений принаймні один аудитор з сертифікації систем управління. Для обґрунтування наявності достатності технічних знань групи аудиту приведено всі необхідні дані в протоколі (Ф-09.01-03).

Примітка. Група може складатися з одного аудитора, за умови, що цей аудитор відповідає всім вимогам до групи з аудиту. Аудитор має виконувати всі належні обов’язки керівника групи аудиту (згідно ДСТУ ISO 19011).

5.6.2 Під час прийняття рішення щодо чисельності та складу групи з аудиту враховуються: цілі аудиту, сферу, критерії аудиту, а також розрахунок тривалості аудиту; складність аудиту та чи є аудит комплексним, інтегрованим або спільним; вибрані методи аудиту; загальна компетентність групи з аудиту, необхідна для досягнення цілей аудиту (згідно QI.07.01); необхідність забезпечення незалежності групи з аудиту від діяльності, що перевіряється та уникнення будь-яких конфліктів інтересів; здатність членів групи з аудиту результативно взаємодіяти і співпрацювати з об'єктом аудиту; мову, яка використовуватиметься під час аудиту і розуміння та культурних особливостей об'єкта аудиту; вимоги сертифікації (охоплюючи будь-які застосовні законодавчі, регуляторні, договірні вимоги, а також інші вимоги, які організація зобов’язується дотримувати), чи члени групи з аудиту раніше проводили аудит системи менеджменту клієнта.

5.6.3 При проведенні сертифікації СУІБ, до вибору групи аудиту та призначення складу, крім вищевикладених вимог, додатково використовують такі вимоги та настанови.

Група аудиту повинна бути формально затверджена та забезпечена відповідними робочими документами. Мандат, який видають групі аудиту, повинен бути чітко визначеним та відомим клієнту. Група аудиту може складатися з однієї особи за умови, що особа відповідає всім встановленим критеріям.

Для підтвердження компетентності групи аудиту використовують вимоги, зазначені в 7.1.2 ДСТУ ISO/IEC 27006.

Для наглядових аудитів і спеціальних аудитів використовують лише ті вимоги, які відповідають запланованим наглядовим діям та діям спеціального аудиту. Якщо вибрана

та керована група аудиту призначена для здійснення спеціального сертифікаційного аудиту, ОС повинен гарантувати, що компетентність для кожного призначення є відповідними.

Група повинна:

a) мати відповідні технічні знання для виконання специфічних дій у межах сфери застосування СУІБ, для якого передбачено сертифікацію, і якщо доречно, з пов'язаними процедурами та їх потенційними ризиками інформаційної безпеки (технічні експерти мають відповідати цій функції);

b) мати розуміння того, що клієнт готовий до здійснення надійного сертифікаційного аудиту його СУІБ для заданої сфери застосування СУІБ та обставин всередині організації в управлінні аспектами інформаційної безпеки його діяльності, продуктів і сервісів;

c) мати відповідне розуміння законодавчих і регуляторних вимог, застосовних до СУІБ клієнта.

Примітка. Відповідне розуміння не забезпечують глибокої законодавчої основи

5.6.4 Цілі аудиту визначає ОС. Сфера та критерії аудиту, включаючи будь-які зміни, встановлюються ОС після аналізу заявки.

Примітка. Керівник групи комплексного або інтегрованого аудиту повинен мати поглиблені знання щонайменше одного зі стандартів та бути ознайомлений з положеннями інших стандартів, що використовуються для конкретного аудиту.

Комплексний аудит – це аудит, при якому проходить аудит заявника на відповідність вимогам двох або більше стандартів щодо систем менеджменту одночасно.

Інтегрований аудит – це аудит, при якому заявник об'єднав застосування вимог двох або більше стандартів на системи менеджменту в єдину систему менеджменту, і аудит якої здійснюють на відповідність більш ніж одного стандарту.

Спільний аудит – це аудит, при якому дві або більше аудиторських організацій співпрацюють з метою проведення аудиту одного заявника.

5.6.5 За необхідності необхідні знання та вміння забезпечується включенням до складу групи з аудиту технічних експертів, письмових та усних перекладачів, які повинні виконувати роботу під керівництвом аудитора. Де використовуються письмові та усні перекладачі, вони обираються таким чином, щоб вони не впливали негативно на аудит. Технічний експерт в групі з аудиту не повинен діяти як аудитор. Технічного експерта має супроводжувати аудитор.

Примітка. Критерії відбору технічних експертів визначаються на індивідуальній основі, виходячи з потреб групи аудиту та сфери аудиту, враховуючи вимоги QI.07.01.

5.6.6 ОС попередньо інформує замовника про персональний склад групи аудиторів з метою надання можливості оскаржити призначення будь-яких конкретних аудиторів чи експертів.

Замовник може вимагати заміни окремих членів групи з аудиту за наявності розумних підстав, виходячи з принципів здійснення аудиту. Розумними підставами є ситуації, пов'язані з конфліктом інтересів або в тому випадку, коли мала місце неетична поведінка в минулому. Про такі підстави повідомляється керівник ОС. Разом з замовником ОС розглядає питання щодо заміни членів групи з аудиту.

5.6.7 Аудитори-стажисти можуть бути включені в групу з аудиту в якості учасників, за умови призначення одного з аудиторів їх оцінювачем. Оцінювач повинен бути компетентним, щоб взяти на себе обов'язки і загальну відповідальність за діяльність та висновки аудитора-стажиста.

5.6.8 Керівник групи аудиту встановлює можливість здійснення аудиту з урахуванням, за необхідності, таких факторів:

- достатності та відповідності інформації для планування аудиту;
- належної співпраці з боку об'єкта сертифікації СУ;
- достатності часу та ресурсів;

- здатності ОС провести сертифікацію СУ відповідно до заявленої номенклатури видів діяльності;

- місцезнаходження об'єктів Замовника, а також будь-яких інших спеціальних вимог, зокрема мови, що нею користується Замовник, загрози неупередженості, умов безпеки.

5.6.9 При визначенні достатності часу, а також дня аудиту, ОС враховує такі чинники: розмір та кількість ділянок, їх географічне розташування та розгалуженість структури (охоплюючи тимчасові робочі місця); пори року (сезону); кількість виробничих ліній, в межах категорій та підкатегорій, охоплених сферою сертифікації; результати будь-яких попередніх аудитів системи управління, і стандарти, які застосовуються при сертифікації; будь-які види діяльності на умовах аутсорсингу, які охоплено сферою системи управління; складність клієнта та його системи управління; технологічні і регуляторні обставини; ризики, пов’язані з продукцією, процесами або видами діяльності організації; чи аудит є скомбінований, спільний або інтегрований; тощо.

5.6.10 У випадку розгалуженої структури, коли застосовується вибірковість аудиту СУ заявника, що охоплює однакові види діяльності на різних ділянках, група з аудиту розробляє програму вибірковості, щоб гарантувати належний аудит СУ (згідно рекомендацій IAF MD 1). Таке обґрунтування документується для кожного замовника.

ОС може відмовити Замовнику в сертифікації за наявності факторів, наведених нижче:

- відсутність комплекту документів, необхідних для проведення робіт з сертифікації;

- фальсифікація документів представлених для експертизи;

- відмова замовника від оплати робіт з сертифікації.

5.6.11 Керівник групи аудиту налагоджує попередній зв'язок з об'єктом аудиту. Метою цього зв'язку є:

- встановлювання способів обміну інформацією з представниками об'єкта аудиту;

- підтвердження повноважень щодо проведення аудиту;

- надання інформації про запропонований термін проведення аудиту, склад групи з аудиту, цілі, сферу, методи аудиту;

- визначення правил безпеки, застосовних на місцях проведення аудиту;

- укладання договору щодо проведення аудиту;

- погодження присутності спостерігачів і потреби у супроводжувальних особах для групи аудиту;

- звернутися із запитом щодо доступу до відповідних документів і протоколів для цілей планування;

- визначити застосовні правові вимоги, а також інші вимоги, доречні для діяльності та продукції об’єкта аудиту;

- підтвердити погодження з об’єктом аудиту ступеня розголошення конфіденційної інформації та поводження з нею;

- вжити організаційних заходів щодо аудиту, зокрема скласти календарний графік;

- визначити сфери, що зацікавлюють або непокоять об’єкта аудиту стосовно конкретного аудиту.

5.6.12 При виникненні ситуації, пов’язаної з конфліктом інтересів (якщо член групи був працівником замовника або надавав йому консультації чи послуги, або проявив себе неетичною поведінкою в минулому тощо), керівник групи з аудиту має розглянути це питання з замовником перед прийняттям рішення щодо заміни членів групи з аудиту.

5.6.13 Керівник групи з аудиту, за погодженням з групою аудиту, встановлює для кожного члена групи відповідальність за проведення аудиту конкретних процесів, функцій, об’єктів, областей або видів діяльності. При цьому враховується незалежність, компетентність та результативне і ефективне використання групи з аудиту, а також різні ролі та обов’язки аудиторів, аудиторів - стажистів та технічних експертів. Щоб

забезпечити досягнення цілей аудиту, під час проведення аудиту керівник групи аудиту може вносити зміни до розподілу обов'язків.

5.6.14 Спостерігачі за попереднім погодженням з замовником, можуть супроводжувати групу з аудит, але вони не входять до її складу і не можуть впливати на проведення аудиту або втручатись в нього.

Примітка. Спостерігачами можуть бути представники органу акредитації, члени організації-клієнта, консультанти, регуляторні органи або інші особи, присутність яких обґрунтована).

5.6.15 Для кожного аудитора заявник повинен надати супроводжувача (особу, яку призначено заявником допомагати групі з аудиту), якщо інше не погоджено між керівником групи з аудиту та заявником.

Супроводжувачі призначаються до групи з аудиту для сприяння проведенню аудиту. Група з аудиту забезпечує, щоб супроводжувачі не впливали або втручались в процес аудиту або результати аудиту.

Примітка. Обов'язки супроводжувача можуть бути наступні: встановлення контактів та координацію часу проведення співбесід; організація візитів до певних частин ділянки або організації; забезпечення того, щоб правила, що стосуються охорони праці на місці та процедур забезпечення безпеки доведені до відома та виконуються членами групи з аудиту; спостерігання за аудитом від імені заявника; надання роз'яснень або інформації на прохання аудитора.

Коли це доречно, особа щодо якої проводять аудит може виступати в ролі супроводжувача.

5.7 Програма аудиту

5.7.1 У разі позитивного рішення за заявкою, компетентна особа ОС розробляє Програму аудиту для повного циклу сертифікації (Ф-09.01-05), яка включає в себе проведення первинного сертифікаційного аудиту у два етапи, наглядові аудити та аудит повторної сертифікації (ресертифікації) на третій рік до закінчення сертифікації.

5.7.2 Перший трирічний цикл сертифікації розпочинається з прийняття рішення щодо сертифікації. Подальші цикли починаються з прийняття рішення щодо повторної сертифікації.

Примітка. При розробці чи перегляді програми аудиту можуть додатково розглядатись наступні фактори: скарги, що надійшли до ОС стосовно заявника; комбінований, інтегрований або комплексний аудит; зміни до вимог сертифікації; зміни законодавства; зміни вимог акредитації; відомості про організаційну результативність; інтереси відповідних зацікавлених сторін.

Примітка. При розробці програми аудиту для багатооб'єктної організації враховуються вимоги QI.09.03 «Порядок застосування вибірки під час проведення аудиту систем управління при розгалуженій структурі».

5.8 Визначення часу аудиту

5.8.1 Відповідальна особа ОС здійснює розрахунок тривалості робіт з сертифікації, а також обґрунтовує вибіркове дослідження згідно вимог QI.09.02 «Порядок оформлення договорів та визначення часу аудиту», враховуючи вимоги IAF MD 1, IAF MD 5, IAF MD 11, та оформлює протокол (Ф-09.01-03).

5.8.2 При визначенні достатності часу аудиту, враховуються такі чинники:

- вимоги відповідного стандарту на системи управління;
- складність заявника та його системи управління;
- технологічні і регуляторні обставини;
- результати будь-яких попередніх аудитів;
- розмір та кількість ділянок, їх географічне розташування та розгалуженість структури;
- ризики, пов'язані з продукцією, процесами або видами діяльності організації;

- будь-які види діяльності на умовах аутсорсингу, які охоплено галуззю системи управління;

- якщо аудит об'єднаний, спільний або інтегрований.

*Примітка***.** Час, витрачений на подорож до та з ділянок, де проходив аудит, не включається до розрахунку тривалості днів аудиту систем управління.

5.8.3 У випадку сертифікації інтегрованої системи управління, розрахунок здійснюється для кожної системи управління.

5.8.4 У випадку розгалуженої структури, коли застосовується вибірковість аудиту СУ заявника, що охоплює однакові види діяльності на різних ділянках, група з аудиту розробляє програму вибірковості, щоб гарантувати належний аудит СУ (згідно рекомендацій IAF MD 1). Таке обґрунтування документується для кожного замовника.

5.9 Попередня оцінка СУ (І етап аудиту)

5.9.1 До здійснення остаточної перевірки та оцінки СУЯ та СУПК група з аудиту здійснює аналіз документації заявника для визначення відповідності задокументованої системи управління критеріям аудиту.

До здійснення остаточної перевірки та оцінки СУІБ, при провадженні стадії 1, ОС повинен отримати документацію щодо побудови СУІБ, яка покриває документацію, визначену в ISO/IEC 27001.

Орган сертифікації повинен отримати достатнє розуміння побудови СУІБ з урахуванням обставин організації клієнта, оцінювання та оброблення ризиків (зокрема й визначені заходи безпеки), політики та цілей інформаційної безпеки й готовність клієнта до аудиту. Це дозволить планувати стадію 2.

Результати стадії 1 повинні бути задокументовані в письмовому звіті. Орган сертифікації повинен переглянути звіт стадії 1 аудиту перед прийняттям рішення про початок стадії 2 і для вибору членів групи аудиту стадії 2 з потрібною компетентністю. Орган сертифікації повинен зробити запит клієнту про подальші типи інформації та записів СУІБ, які можуть бути потрібні для детальної перевірки СУІБ протягом стадії 2.

5.9.2 Під час аналізування документації група з аудиту враховує розмір, характер діяльності і складність організації, а також цілі та сферу аудиту. У деяких випадках це аналізування може бути відкладено до початку робіт на місцях, якщо це негативно не впливатиме на результативність проведення аудиту. В інших випадках може бути здійснене попереднє відвідування місць проведення аудитів з тим, щоб мати відповідне уявлення про наявну інформацію. Місця проведення попереднього аналізування документації визначає керівник групи аудиту (Під час попереднього оцінювання документації СУ воно може здійснюватися як у замовника, так і в ОС).

5.9.3 Процедура проведення попередньої оцінки СУ на підприємстві проводиться ідентично остаточній перевірці з метою:

- перевірити задокументовану інформацію СУ замовника;

- щоб оцінити розташування замовника і специфічні умови розташувань ділянок, і провести обговорення з персоналом замовника з метою визначення готовності до другого етапу аудиту;

- щоб проаналізувати стан замовника і його розуміння щодо вимог стандарту, зокрема стосовно визначення ключових характеристик або суттєвих аспектів, процесів, цілей і функціювання СУ;

- щоб зібрати необхідні відомості щодо сфери СУ, включаючи: ділянки(нок) заявника; процеси та обладнання; встановлені рівні контролю; застосовні законодавчі та регуляторні вимоги;

- щоб проаналізувати розподіл ресурсів для проведення аудиту другого етапу, погодити з замовником деталі аудиту другого етапу та забезпечити конкретизацію планування остаточного аудиту;

- щоб забезпечити конкретизацію планування аудиту другого етапу завдяки досягненню достатнього розуміння СУ заявника і діяльності його дільниць в контексті стандарту на СУ або інших нормативних документів;

- щоб оцінити, чи плануються і виконуються внутрішні аудити і аналізування керівництвом і що ступінь впровадження СУ підтверджує, що замовник готовий до аудиту другого етапу;

5.9.4 Група з аудиту організує збір додаткових відомостей про якість продукції, стосовно якої проводяться роботи з сертифікації СУ, від незалежних джерел.

Отримані дані документуються і повідомляються замовнику, включаючи визначення будь-яких ділянок, що викликають занепокоєння та, які можуть бути кваліфіковані як невідповідність під час остаточного аудиту.

5.9.5 У випадку проведення попередньої оцінки першого етапу первинної сертифікації на місці, керівник групи аудиту складає графік аудиту, на початку аудиту проводить вступну нараду, за участю представників заявника, по закінченні аудиту - заключну нараду.

5.9.6 Попередня оцінка системи управління заявника завершується підготовкою письмового висновку (Ф-09.01-07) по результатах попередньої оцінки, який містить оцінку відповідності задокументованої СУ вимогам відповідного стандарту та рішення щодо доцільності або недоцільності проведення остаточної перевірки і оцінки системи управління (II етапу аудиту). Висновок готується у двох примірниках: один залишається в ОС, другий передається заявнику.

5.9.11 У разі виявлення невідповідностей за результатами I етапу аудиту у висновку наводяться усі виявлені невідповідності СУ вимогам сертифікації, також мають бути визначені будь-які проблемні зони, які може бути класифіковано як невідповідність під час 2-го етапу аудиту. Після чого приймається рішення або щодо продовження аудиту, або його тимчасового припинення на термін приведення документації у відповідність вимогам застосовного стандарту. Заявником за погодженням з ОС визначається термін для усунення виявлених невідповідностей, але не більше 6-х місяців. При визначенні інтервалу між попереднім і остаточним аудитами необхідно прийняти до уваги потреби замовника вирішити проблемні питання, які були встановлені при попередньому аудиті.

ОС інформує замовника, що результати I етапу аудиту можуть призвести до відкладення або скасування II етапу аудиту.

5.9.12 В залежності від кількості виявлених невідповідностей за результатами попереднього оцінювання СУ ОС може прийняти одне з нижченаведених рішень:

- у разі виявлення значної кількості невідповідностей, проведення остаточної перевірки та оцінки СУ є недоцільним. Подальші роботи з сертифікації СУ призупиняються до усунення заявником виявлених невідповідностей. Після того, як заявник надасть переконливі докази стосовно усунення всіх виявлених невідповідностей ОС проводить повторну оцінку документації СУ заявника з укладанням додаткового договору. Вартість цих робіт визначається з урахуванням фактичних витрат часу групи з аудиту на повторне оцінювання. За результатами повторного оцінювання складається висновок стосовно відповідності документації СУ заявника вимогам використовуваного стандарту.

- у разі незначної кількості невідповідностей і усунення їх заявником без внесення суттєвих змін до СУ для їх усунення, ОС приймає рішення про доцільність проведення робіт з сертифікації СУ, у разі усунення невідповідностей до проведення остаточної перевірки та оцінки СУ. Роботи з попереднього повторного оцінювання проводяться без укладання додаткового договору. При цьому аналізуються тільки ті процеси, стосовно яких були виявлені невідповідності.

5.9.13 Після підписання висновку за результатами попередньої оцінки керівник групи аудиту інформує зацікавлені сторони щодо подальшого проведення аудиту.

ОС може не проводити 2-й етап аудиту, повідомивши про це замовника, у випадку:

- якщо протягом визначеного терміну замовником не надано докази усунення невідповідностей, виявлених при проведенні 1-го етапу аудиту;

- якщо організація порушує умови договору.

5.10 Остаточна перевірка та оцінка СУ

5.10.1 Остаточна перевірка і оцінка системи управління – II етап аудиту, здійснюється групою з аудиту під керівництвом керівника групи аудиту.

5.10.2 За результатами аналізу документів та висновку попереднього аудиту керівник групи аудиту готує план аудиту з графіком аудиту (Ф-09.01-08), як основу забезпечення згоди між замовником, групою з аудиту та об'єктом сертифікації, стосовно проведення аудиту. Графік є невід'ємною частиною плану аудиту.

План та графік аудиту охоплюють:

- цілі аудиту;
- критерії аудиту;
- сферу аудиту, зокрема ідентифікацію організаційних та функціональних одиниць або процесів, які підлягатимуть аудиту;
- дати і місця, де буде проводитись аудит на місці, зокрема відвідування тимчасових об'єктів та діяльність з дистанційного аудиту, якщо це застосовно, включаючи вступну та заключну наради з керівництвом об'єкта аудиту;
- очікувана тривалість аудиторської діяльності на місці;
- ролі та обов'язки членів групи з аудиту та супроводжуючих осіб, таких як спостерігачі або перекладачі.

При складанні графіка аудиту керівник групи з аудиту за участі членів групи з аудиту повинен проаналізувати застосовані до відповідного підприємства законодавчі, регуляторні та договірні вимоги та додати окремим розділом до графіка аудиту перевірку цих вимог.

Якщо в організації функціонують декілька систем управління, до плану аудиту можуть бути включені скомбіновані аудити. Якщо організація має декілька філій, розташованих у різних місцях, але які виконують однакові функції, керівник групи аудиту вказує в графіку аудиту, в якій саме філії буде проведено аудит.

Обґрунтування часу аудиту та ділянок, де проводиться аудит (якщо підприємство має розгалужену структуру) вказується в протоколі (Ф-09.01-03) та плані аудиту (Ф-09.01-08).

5.10.3 Обсяг плану аудиту (Ф-09.01-08) залежить від галузі та складності системи управління замовника, розміру, характеру діяльності та складності організації, аудит якої проводиться, а також від: кількості, важливості, складності, подібності та місцезнаходження видів діяльності, які підлягають аудиту; законодавчих, регламентувальних і контрактних вимог та інших критеріїв аудиту; висновків попередніх аудитів або результатів аналізування попередньої програми/плану аудиту; інтересів зацікавлених сторін; суттєвих змін в організації або в її діяльності.

5.10.4 Керівник групи аудиту після ознайомлення членів групи з аудиту з планом аудиту, погоджує його з замовником аудиту та надає об'єкту аудиту до початку аудиторської діяльності на місцях. Спірні питання щодо змісту плану в цілому, або деяких його пунктів, мають бути вирішені між керівником групи аудиту, об'єктом аудиту та замовником аудиту. Будь-які зміни плану аудиту узгоджуються з зацікавленими сторонами до початку аудиту. Після проведення аудиту керівник групи аудиту здійснює аналіз плану аудиту з метою встановлення, чи досягнуто його цілі та чи є необхідність поліпшення.

5.10.5 Для реалізації плану аудиту і відображення його результатів щодо конкретних розділів, члени групи з аудиту здійснюють перевірки закріплених за ними об'єктів перевірки шляхом опитувань, вивчення документів та здійснення спостережень на ділянках відповідно до графіку аудиту.

Завдання групи з аудиту, які визначені в плані аудиту та в графіку аудиту вимагають від групи з аудиту:

- дослідити та перевірити структуру, політики, процеси, процедури, записи і пов'язані

документи клієнта відповідно до стандарту на систему менеджменту;

- визначити, чи задовольняють вони всі вимоги, відносно заявленої сфери сертифікації;

- визначити, чи розроблені, запроваджені та ефективно підтримуються процеси і процедури, з метою забезпечення основи для довіри до системи менеджменту заявника;

- повідомляти заявнику, для його реагування, щодо будь-якої неузгодженості між політикою, завданнями і цілями підприємства - заявника.

5.10.6 План та графік аудиту розробляється керівником групи з аудиту з урахуванням положень ДСТУ ISO 19011. Рівень деталізації інформації, наданої в плані аудиту, відповідає сфері та складності аудиту.

5.10.7 План та дата аудиту погоджується з об'єктом аудиту та замовником аудиту до початку проведення остаточної перевірки та оцінки СУ.

5.10.8 При проведенні остаточної перевірки та оцінки СУ можливе внесення змін в графік аудиту за згодою зацікавлених сторін.

5.10.9 Усі спостереження, зроблені під час остаточної перевірки та оцінки СУ, члени групи з аудиту відображають в робочих документах (Чек-листи, які зберігаються до кінця аудиту), протоколи невідповідностей, протоколи нарад.

5.10.10 Для здійснення сертифікації СУІБ, на основі висновків, задокументованих у висновку (Ф-09.01-07) етапу 1 аудиту, ОС розробляє план (Ф-09.01-08) для виконання етапу 2.

Додатково до оцінювання ефективності впровадження СУІБ, цілями етапу 2 будуть:

a) підтвердження, що клієнт дотримується своїх власних політик, цілей та процедур.

Зробивши це, аудит повинен сконцентруватися на:

a) провідній ролі та зобов’язаннях вищого керівництва клієнта стосовно політики інформаційної безпеки та цілей інформаційної безпеки;

b) вимогах документації, зазначених в ISO/IEC 27001;

c) оцінюванні ризиків, пов’язаних з інформаційною безпекою, і тому, що оцінювання призводить до постійних, цінних і порівняних результатів, якщо його виконують повторно;

d) визначенні цілей заходів безпеки та заходів безпеки, основаних на оцінці ризиків інформаційної безпеки та процесів оброблення ризиків;

e) результативності інформаційної безпеки та ефективності СУІБ у разі зіставляння з цілями інформаційної безпеки;

f) відповідності між визначеними заходами безпеки, Положенням щодо застосовності та результатами оцінки ризиків інформаційної безпеки і процесу оброблення ризиків та політики і цілей інформаційної безпеки;

g) впровадженні заходів безпеки з урахуванням внутрішніх та зовнішніх обставин і пов’язаних ризиків, моніторингу, вимірювань та аналізу процесів інформаційної безпеки й заходів безпеки для визначення того, чи були заходи безпеки впроваджені та ефективні і чи відповідають зазначеним цілям інформаційної безпеки;

h) ефективності програм, процесів, процедур, записів, внутрішнього аудиту й переглядів СУІБ для гарантування того, що вони відповідають рішенням вищого керівництва та політиці і цілям інформаційної безпеки.

5.11 Здійснення аудиторської перевірки на місцях

5.11.1 Другий етап аудиту проводиться безпосередньо на місці розташування заявника.

5.11.2 У випадку, коли будь-яка частина аудиту проводиться за допомогою електронного устаткування або ділянка, аудит якої необхідно провести є віртуальною, ОС

здійснює підбір групи аудиту із відповідною компетентністю. Докази, отримані під час такого аудиту повинні бути достатніми щоб дозволити аудитору прийняти обґрунтоване рішення щодо відповідності вимогам, що перевіряються.

5.11.3 Керівник аудиторської групи проводить попередню нараду. У ній беруть участь члени групи аудиту, керівництво замовника та, за необхідності, відповідальні за діяльність чи процеси, які підлягають аудиту.

Метою наради є:

- підтвердження плану та графіку аудиту ;
- подання стислого опису того, як буде проведено аудит;
- підтвердження способів обміну інформацією;
- надання можливості персоналу об'єкта аудиту задати запитання.

На попередній нараді розглядаються такі питання:

- представлення учасників з окресленням їх ролей;
- підтвердження цілей, сфери та критеріїв аудиту;
- підтвердження плану та графіку проведення аудиту (зокрема, тип і сферу аудиту, його цілі і критерії), будь-яких змін та інших відповідних домовленостей з об’єктом аудиту, таких як дата і час проведення заключної наради, проміжних нарад групи з аудиту та керівництва об’єкта аудиту;
- методи і процедури, які використовуватимуть під час проведення аудиту на основі вибірки, а також доведення до відома об'єкта аудиту, що доказ аудиту базуватиметься лише на частині наявної інформації і тому для аудита є характерним елементом невизначеності;
- підтвердження офіційних способів обміну інформацією між групою з аудиту і об’єктом аудиту;
- підтвердження мови, яку використовуватимуть під час аудиту;
- підтвердження того, що під час аудиту, об'єкт аудиту отримуватиме всю інформацію про хід виконання аудиту та будь-які проблемні питання;
- підтвердження наявності ресурсів і забезпеченості умовами роботи необхідних груп з аудиту;
- підтвердження того, що є предметом конфіденційності;
- підтвердження відповідних дій, пов'язаних з охороною праці, аварійними ситуаціями та особистою безпекою для груп з аудиту;
- підтвердження наявності, ролей та особистостей будь-яких супроводжувальних осіб та спостерігачів;
- метод звітування, включаючи градацію даних аудиту;
- інформацію про умови, за яких аудит може бути достроково припинений;
- інформацію про порядок подання апеляцій стосовно проведення аудиту чи його висновків;
- підтвердження того, що керівник групи з аудиту та група з аудиту, яка представляє ОС, несе відповідальність за аудит і буде контролювати виконання плану та графіку аудиту, охоплюючи діяльність з аудиту та записи аудиту;
- підтвердження статусу даних попереднього аналізування або аудиту, за наявності.

5.11.4 За результатами попередньої наради складають протокол (Ф-09.01-09).

5.11.5 Група з аудиту проводить оцінку системи управління об'єкта аудиту на відповідність встановлених критеріїв аудиту.

Під час аудиту проводиться збір інформації згідно з цілями, сферою та критеріями аудиту, включаючи:

- інформацію і докази відповідності всім вимогам використовуваного стандарту на систему управління або іншого нормативного документу;

- здійснення моніторингу, вимірювання, звітування і аналізування на відповідність ключовим завданням і цілям (узгоджених з очікуванням у застосовуваному стандарті системи управління або іншому нормативному документі);

- дотримання системою менеджменту замовника і його діяльністю застосовних законодавчих, регуляторних та договірних вимог;

- інформацію щодо зв'язків між видами діяльності, процесами та її перевірка; проведення внутрішнього аудиту та аналізування з боку керівництва;

- інформацію стосовно відповідальності керівництва замовника за власну політику;

- інформацію стосовно зв'язків між нормативними вимогами, політикою, завданнями та цілями (сумісними з очікуваннями у застосовному стандарті системи управління або іншому нормативному документі), будь-якими застосовними законодавчими вимогами, обов'язками, компетентністю персоналу, процесами, процедурами, показниками роботи і даними внутрішнього аудиту і рішеннями;

- оперативне керування процесами заявника.

5.11.6 Група аудиту повинна повідомити замовнику про його дії, будь-які несумісності між політикою замовника, цілями і метою (що відповідають очікуваннями відповідного стандарту на систему менеджменту або іншому нормативному документу) і результати. Лише інформація, яку можна перевірити є доказом аудиту.

5.11.7 Методи збирання інформації містять: співбесіди, спостереження за процесами та діяльністю, аналізування документації та записів.

5.11.8 Під час аудиту керівник групи з аудиту, у разі необхідності, проводить наради для обміну інформацією, оцінювання ходу виконання аудиту і перерозподілу, у разі потреби, робочих завдань між членами групи з аудиту.

Під час аудиту керівник групи з аудиту періодично інформує об'єкт аудиту і, за необхідності, замовника аудиту про хід виконання аудиту та будь-які проблеми.

5.11.9 Для підготування даних аудиту оцінюються докази аудиту за критеріями аудиту. Невідповідності, виявлені при проведенні перевірки та оцінки СУ реєструються в протоколах невідповідностей (Ф-09.01-15). Невідповідності аналізуються за участю об'єкта аудиту для отримання визнання того, що доказ аудиту є правильним і невідповідності є зрозумілими.

5.11.10 У разі, коли наявний доказ аудиту свідчить про неможливість досягнення цілей аудиту, керівник групи з аудиту доповідає про причини цього замовнику аудиту і об'єкту аудиту для визначення відповідної дії.

5.11.11 Супроводжувальні особи і спостерігачі можуть супроводжувати групу з аудиту, але вони не входять до її складу. Вони не повинні впливати на проведення аудиту або втручатися в нього.

Супроводжувальні особи можуть бути відповідальними за:

- встановлення контактів і часу для опитування;

- підготування відвідування конкретних місць організації або організації в цілому;

- ознайомлення членів групи з аудиту з правилами охорони праці та особистої безпеки і їх дотримання;

- засвідчення результатів аудиту від імені об'єкта аудиту;

- надання пояснень чи допомоги у збиранні інформації.

Вибрані джерела інформації можуть різнитися залежно від сфери та складності аудиту і можуть містити:

- опитування працівників та інших осіб;

- спостереження за діяльністю, виробничим середовищем та умовами;

- документи, такі, як політика, цілі, плани, методики, стандарти, інструкції, ліцензії та дозволи, технічні умови, креслення, контракти і замовлення;

- протоколи, такі, як протоколи контролю, протоколи нарад, звіти про аудит, протоколи за програмами моніторингу і результати вимірювання;

- зведені дані, результати аналізування і показники діяльності;

- інформацію про програми об'єкта аудиту щодо відбирання зразків і про методики з управління процесами відбирання зразків та вимірювання;

- повідомлення з інших джерел, наприклад, зворотній зв'язок із замовниками, іншу відповідну інформацію від зовнішніх сторін та рейтинг постачальників;

- комп'ютерні бази даних і веб-сайти.

Опитування проводиться у спосіб, прийнятний для ситуації та особи, яку опитують. При опитуванні враховується те, що:

- опитування необхідно проводити з особами відповідних рівнів та функціональних обов'язків у межах сфери аудиту;

- опитування слід проводити у звичайний робочий час і, якщо можливо, на робочому місці особи, яку опитують;

- до початку та під час опитування треба докладати усіх зусиль для створення невимушеної атмосфери для особи, яку опитують;

- треба пояснювати причину опитування та необхідність ведення будь-яких записів;

- опитування може починатися з прохання до осіб розповісти про свою роботу;

- треба уникати запитань, що впливають на відповідь;

- результати опитування треба підсумовувати та переглядати за участю особи, яку опитували;

- треба подякувати особам, яких опитували, за їхню участь та співпрацю.

5.11.12 На відповідних стадіях здійснення аудиту група з аудиту збирається для аналізу отриманих даних.

Відповідність даних аудиту критеріям аудиту підсумовується із зазначенням місць, функцій або процесів, аудит яких було проведено. Невідповідності аналізуються за участю об'єкта аудиту для отримання визнання того, що доказ аудиту є правильним і невідповідності є зрозумілими («Зрозумілими» не обов’язково означає, що невідповідності були визнані об’єктом аудиту). Члени групи з аудиту повинні докладати всіх зусиль для узгодження думок стосовно доказу аудиту і (або) даних аудиту, а всі розбіжності необхідно реєструвати у протоколах реєстрації невідповідностей. Невідповідності класифікують як значні та незначні.

5.11.13 Перед проведенням заключної наради група з аудиту проводить нараду з тим, щоб: проаналізувати зібрані під час аудиту дані аудиту та будь-яку іншу відповідну інформацію на відповідність цілям аудиту; дійти згоди щодо висновків аудиту, враховуючи притаманну процесу аудиту невизначеність; визначити будь-які необхідні подальші дії; підтвердити доцільність плану аудиту або визначити будь-які необхідні зміни для майбутніх аудитів (наприклад, щодо сфери, тривалості або дати аудиту, частоти наглядань, компетентності групи з аудиту).

5.11.14 У результаті перевірки та оцінки СУ можливі такі основні висновки:

СУ повністю відповідає критеріям аудиту (варіант 1);

СУ в цілому відповідає критеріям аудиту, але виявлено невідповідності, які можуть бути усунуті досить швидко (варіант 2);

СУ має критичні невідповідності, які можна усунути лише в результаті доопрацювання протягом досить тривалого часу (варіант 3).

5.11.15 Заключна нарада проводиться під головуванням керівника групи з аудиту для представлення даних аудиту та висновків аудиту таким чином, щоб їх зрозумів та підтвердив об'єкт аудиту.

5.11.16 В протоколі заключної наради (Ф-09.01-10) відображають висновки щодо відповідності СУ за результатами сертифікаційного аудиту, включаючи наступні дані:

- повідомити об’єкту аудиту, що зібрані докази в ході аудиту були засновані на вибірці інформації, тим самим спричинивши елемент невизначеності;

- визначення способу та термінів звітування, зокрема будь-якої градації результатів аудиту;

- інформація стосовно процесу органу з сертифікації щодо поводження з невідповідностями, зокрема, будь-які наслідки, пов'язані із статусом сертифікації об’єкта аудиту;

- визначаються терміни представлення плану коригування та коригувальних дій щодо будь-яких невідповідностей, виявлених під час аудиту;

- інформація стосовно дій ОС після аудиту;

- інформація щодо процесів вирішення скарг та розглядання апеляцій.

- СУ відповідає вимогам відповідного стандарту;

- СУ має невідповідності,

- а також пропозиції щодо надання чи ненадання сертифікації та умови надання чи будь-які зауваження.

5.11.17 Якщо при проведенні 2-го етапу аудиту виявлено невідповідності, то при проведенні заключної наради керівник групи аудиту повідомляє про це керівництво організації і погоджує термін, в який організація повинна здійснити коригування/коригувальні дії та надати документовані докази стосовно їх виконання до ОС. Організація, об’єкт аудиту, повинна розробити План виконання коригувальних дій, в якому вказуються заходи для усунення виявлених невідповідностей, відповідальні та терміни усунення невідповідностей.

ОС проводить перевірку виконання таких дій з відвідуванням або без відвідування підприємства.

При проведенні заключної наради керівник групи аудиту повідомляє, що зібрані докази в ході аудиту були засновані на вибірковості інформації, тим самим вводиться елемент невизначеності. Також надає інформацію щодо розгляду скарг та апеляцій.

5.11.18 Проведення заключної наради оформляється протоколом (Ф-09.01-10) з реєстрування усіх присутніх. Під час проведення заключної наради група з аудиту узгоджує з керівництвом об'єкта аудиту термін підготовки звіту про перевірку.

5.11.19 Всі протоколи нарад оформлюються в 2 примірниках, один з яких зберігається в ОС, а другий надається об'єкту аудиту.

5.11.20 Всі сторони, що зберігають протоколи за результатами перевірки, мають забезпечити нерозголошення конфіденційної інформації щодо результатів перевірки.

5.12 Підготування, схвалення та розсилання звіту про аудит

5.12.1 Відповідальним за підготування звіту про аудит (Ф-09.01-11) та за його зміст є керівник групи з аудиту. Звіт про аудит повинен забезпечити повний, точний, стислий та чіткий опис проведеного аудиту і повинен містити або посилатися на:

- ідентифікацію органу з сертифікації;

- назву та адресу клієнта, та представника клієнта;

- тип аудиту (наприклад, первинний, наглядовий або аудит повторної сертифікації або спеціальні аудити);

- критерії та цілі аудиту;

- сферу аудиту, зокрема, визначення організаційних або функціональних підрозділів чи процесів, аудит яких проведено, а також час проведення аудиту;

- будь-які відхилення від плану та графіку аудиту та їх причини та будь-які значні питання, що впливають на програму аудиту;

- ідентифікацію керівника групи з аудиту, членів групи з аудиту та супроводжуючих осіб;

- дати і місця, де був проведений аудит (на місці або поза ним, постійні або тимчасові ділянки);

- результати аудиту, посилання на докази та висновки аудиту, які б відповідали вимогам даного типу аудиту;

- значні зміни, якщо такі є, що негативно вплинули на систему менеджменту об’єкта аудиту з часу проведення останнього аудиту;

- будь-які невирішені питання, за наявності;

- чи є аудит спільним, комплексним або інтегрованим, якщо застосовно;

- застережна заява про те, що проведення аудиту ґрунтується на процесі вибірки доступної інформації;

- рекомендації від групи з аудиту;

- ефективність, з якою клієнт, аудит якого було проведено, контролює використання документів про сертифікацію та знаків, якщо це застосовно;

- перевірка ефективності запроваджених коригувальних дій стосовно невідповідностей, встановлених раніше, якщо це застосовно.

- заяву про відповідність та ефективність системи менеджменту разом з підсумком доказів, що відносяться до: можливості системи менеджменту відповідати застосовним вимогам та очікуваним результатам; внутрішні аудити та процес аналізу з боку керівництва; висновок щодо прийнятності сфери сертифікації; підтвердження того, що цілі аудиту було досягнуто.

5.12.2 Вимоги до звіту аудиту СУІБ.

Додатково до вимог для звітування, наведених вище, звіт аудиту СУІБ повинен надавати таку інформацію або посилатися на неї:

a) звіт аудиту, зокрема й короткий опис огляду документів;

b) звіт сертифікаційного аудиту стосовно аналізу ризиків інформаційної безпеки клієнта;

c) відхилення від плану аудиту (наприклад, більша чи менша тривалість запланованих дій);

d) сфера застосування СУІБ.

Звіт аудиту повинен бути достатньо детальним для обґрунтування та підтримки рішень щодо сертифікації.

Він повинен містити:

a) змістовний журнал аудиту і застосовану методику аудиту;

b) зроблені спостереження, як позитивні (наприклад, характеристики, які варті уваги), так і негативні (наприклад, потенційні невідповідності);

c) коментарі стосовно відповідності СУІБ клієнта сертифікаційним вимогам з чітким визначенням невідповідності, посиланням на версію Положення щодо застосовності та, де це прийнятно, будь-якими потрібними порівняннями з результатами попередніх сертифікаційних аудитів клієнта.

Заповнені опитувальні анкети, контрольні листи, спостереження, logs-журнали чи нотатки аудитора можуть формувати інтегральну частину звіту аудиту. Якщо ці методи використовують, то ці документи повинні бути надані до органу сертифікації як доказ, який підтримує рішення щодо сертифікації. Інформація стосовно вибірок, оцінених протягом аудиту, повинна бути долучена до звіту аудиту або іншої документації.

Звіт повинен розглядати адекватність внутрішньої організації та процедур, застосованих клієнтом, для отримання впевненості в СУІБ.

Додатково до вимог для звітування, зазначених вище, звіт повинен містити:

- короткий опис найважливіших спостережень, позитивних, а також негативних, стосовно впровадження та ефективності вимог СУІБ та заходів інформаційної безпеки;

- рекомендації групи аудиту, чи треба сертифікувати СУІБ клієнта або ні разом з інформацією задля обґрунтування цієї рекомендації.

5.12.3 Кожний член групи з аудиту подає в звіт дані про стан тих об’єктів системи управління підприємства, які він перевіряв. Звіт підписують усі члени групи з аудиту. Термін підготовки звіту - протягом місяця після проведення заключної наради. Якщо це неможливо, про причини затримки керівник групи з аудиту повідомляє замовника аудиту та погоджує новий термін.

Якщо в термін до одного місяця (під час написання звіту про аудит) об’єкт аудиту надає керівнику групи аудиту докази виконання коригувань/коригувальних дій і група аудиту впевниться в їх результативності, то група з аудиту має відобразити результати

оцінювання у звіті про аудит та пропонувати ОС видати сертифікат на СУ. Якщо для усунення невідповідностей та виконання коригувальних дій для організації необхідно більше одного місяця для виконання коригувальних дій, то у звіті необхідно вказувати фактичний стан усунення невідповідностей та пропозиції стосовно надання сертифікації.

5.12.4 Звіт про аудит розсилається одержувачам, зазначеним в «Плані аудиту» (Ф-09.01-08). Звіт про аудит є власністю ОС.

Примітка. Перевіряння результативності коригування та коригувальної дії може бути здійснено на основі аналізування документації, наданої об'єктом аудиту, або, у випадку необхідності, шляхом перевіряння на місці. Такі дії можуть проводитися членом групи з аудиту.

5.13 Рішення щодо сертифікації

5.13.1 Сертифікат на СУ може бути виданий тільки при відповідності СУ замовника вимогам відповідного стандарту (після усунення невідповідностей та впровадження коригувальних дій і надання переконливих доказів щодо їх впровадження до ОС).

5.13.2 Рішення щодо надання або відмови у сертифікації, розширення або скорочення сфери сертифікації, призупинення або поновлення сертифікації, скасування сертифікації та надання повторної сертифікації приймається особами, які не брали участі в оцінюванні системи управління, а також які повинні мати відповідну компетентність, згідно вимог QI.07.01. З фахівцями, які не є співробітниками ОС, і призначені ОС на прийняття рішення щодо сертифікації підписується угода. Порядок визначення компетентності залученого персоналу згідно вимог QI.07.01.

5.13.4 Призначена компетентна особа, яка приймає рішення стосовно надання сертифікації, розширення або скорочення сфери сертифікації, надання повторної сертифікації, призупинення або поновлення, або скасування сертифікації повинна провести аналіз стосовно:

- інформація, що надана групою з аудиту, є достатньою стосовно вимог сертифікації та сфери сертифікації;
- аналізу, визнання і перевірки коригування і коригувальних дій для будь-яких суттєвих невідповідностей;
- аналізу і прийняття запланованих клієнтом коригувань і коригувальних дій щодо будь-яких несуттєвих невідповідностей.

5.13.5 Інформація, яку надає група з аудиту до ОС для прийняття рішення щодо сертифікації, повинна, щонайменше, охоплювати: звіт про аудит; коментарі щодо невідповідностей і, де це застосовно, коригувань і коригувальних дій, запроваджених об'єктом аудиту; підтвердження наданої ОС інформації, яку використовували під час аналізування заявки; підтвердження того, що цілі аудиту були виконані; рекомендацію щодо надання або ненадання сертифікації, разом з будь-якими умовами або спостереженнями.

5.13.6 У разі позитивного рішення щодо сертифікації (варіант 1) ОС оформлює рішення (Ф-09.01-12) про можливість видачі сертифікату на систему управління (Ф-09.01-13), оформляє ліцензійну угоду (Ф-09.01-14) у двох примірниках на право користування сертифікатом відповідності, яка підписується ОС та замовником та посилається на Програму аудиту для повного циклу сертифікації (Ф-09.01-05), де встановлено відповідні положення та вимоги до наглядових аудитів. В ліцензійній угоді зазначені умови використання сертифікату відповідності на СУ, визначені права і обов'язки Замовника та ОС, використання назви органу з сертифікації. Сертифікат відповідності діє протягом терміну дії угоди. Припинення дії угоди одночасно означає припинення дії сертифікатів відповідності.

5.13.7 Зареєстрований сертифікат на систему управління видається на термін до 3 років.

Трирічний цикл сертифікації починається з рішення щодо видачі сертифікату або рішення щодо ресертифікації.

5.13.8 Реєстрація сертифікатів відповідності на систему управління здійснюється в “Журналі реєстрації заявок та видачі сертифікатів на системи управління”, який ведеться в електронному вигляді.

5.13.9 У разі наявності невідповідностей, які не були своєчасно усунені (варіант 2) то сертифікат на СУ не видають. Замовник після виконання необхідних коригувальних дій повідомляє ОС про необхідність повторного оцінювання СУ.

Керівник групи аудиту визначає обсяг проведення повторного оцінювання, яке може бути проведене за повною чи скороченою схемою:

- якщо в термін від дня 2-го етапу сертифікаційного аудиту пройшло менше 6-ти місяців, організація-заявник подає до ОС заявку на повторне оцінювання СУ, то повторне оцінювання проводиться за скороченою схемою, тобто перевіряються лише ті процеси, стосовно яких були виявлені невідповідності. За позитивними результатами такого оцінювання ОС ухвалює рішення щодо видачі сертифікату на СУ. Про рішення, прийняте ОС повідомляється підприємство.

5.13.10 Якщо ОС не має можливості перевірити впровадження коригувань та коригувальних дій щодо будь-яких суттєвих невідповідностей протягом 6 місяців після останнього дня другого етапу аудиту, ОС проводить ще один другий етап аудиту перед наданням рекомендацій щодо сертифікації.

5.13.11 Організація здійснює оплату робіт з повторного оцінювання за окремим договором.

5.13.12 У разі негативного висновку (варіант 3) групи з аудиту, який наведено в звіті, сертифікат на систему управління не видається. Після доопрацювання системи управління та усунення невідповідностей підприємство має право звернутись повторно до ОС з оформленням нової заявки відповідно 5.1 цього Порядку.

5.13.13 Термін дії сертифікату на систему управління не продовжується. Щоб отримати сертифікат на новий термін дії, клієнт подає в ОС заявку (за 3 місяці до закінчення терміну дії сертифікату). Порядок ресертифікації системи управління клієнта визначається ОС при розгляді заявки в кожному конкретному випадку з урахуванням результатів наглядового аудиту за сертифікованою системою управління протягом дії сертифікації та скарг, отриманих від користувачів сертифікації.

5.13.14 ОС анулює сертифікат на систему управління замовника в разі некоректних посилань на статус сертифікації або оманливого застосування сертифікаційних документів.

5.13.15 В ОС не передбачається трансфер сертифікації.

6 НАГЛЯДОВИЙ АУДИТ ЗА СЕРТИФІКОВАНИМИ СИСТЕМАМИ УПРАВЛІННЯ

6.1 ОС здійснює періодичне наглядання за системою управління протягом усього терміну дії сертифіката, через встановлені проміжки часу, для підтвердження того, що об'єкти аудиту, система управління яких була сертифікована, продовжують відповідати вимогам сертифікації.

6.2 Періодичність проведення наглядового аудиту встановлюється ОС за письмовою пропозицією в звіті групи з аудиту під час проведення сертифікації системи управління. За рішенням ОС періодичність процедур нагляду може змінюватися з урахуванням результатів проведених робіт з сертифікації, терміну дії сертифіката в залежності від складності продукції, імовірності виникнення небезпеки від її використання для життя та здоров'я людини, навколишнього середовища.

6.3 Обсяг і порядок проведення наглядового аудиту за сертифікованими системами управління регламентовано QI.09.04 «Порядок планування та проведення наглядового аудиту за сертифікованими системами управління».

6.4 Наглядові аудити (технічний нагляд) - це аудити на місці, але не обов'язково повні аудити системи управління, і плануються разом з рештою діяльності з наглядання таким чином, щоб ОС був в змозі підтверджувати, що сертифікована система управління

замовника продовжує відповідати вимогам у періоди між повторними сертифікаційними аудитами.

6.5 Наглядовий аудит охоплює:

- внутрішні аудити і аналізування керівництвом;
- перевірку дій, ужитих за результатами невідповідностей, що виявлені протягом попереднього аудиту;
- розгляд скарг;
- результативність системи менеджменту щодо досягнення цілей сертифікованого замовника;
- хід виконання запланованих дій, що направлені на постійне поліпшення;
- постійний оперативний контроль;
- перевірка будь-яких змін, і
- використовування знаків та/або будь-яких інших посилань на сертифікацію.

6.6 Наглядові дії за сертифікованою СУІБ

6.6.1 Процедури наглядового аудиту СУІБ повинні відповідати процедурам сертифікаційного аудиту СУІБ замовника.

Ціллю нагляду є підтвердження, що схвалена СУІБ продовжує впроваджуватися чи функціонувати, розгляд залучених змін до цієї системи, які були ініційовані як результат змін в роботі замовника та підтвердження продовження відповідності вимогам сертифікації.

6.6.2 Програми наглядового аудиту за сертифікованою СУІБ повинні включати хоча б таке:

a) елементи підтримки системи, такі як оцінку ризиків інформаційної безпеки та підтримку заходів безпеки, внутрішні аудити СУІБ, перегляд з боку керівництва та коригувальні дії;

b) зв'язки із зовнішніми сторонами, як цього визначено СУІБ в ДСТУ ISO/IEC 27001, та інші документи, потрібні для сертифікації;

c) зміни в задокументованій системі;

d) сфери, які підлягають змінам;

e) вибрані вимоги ISO/IEC 27001;

f) інші вибрані питання, за наявності.

6.6.3 Кожний нагляд з боку ОС повинен переглядати щонайменше таке:

a) ефективність СУІБ по відношенню до досягнення цілей політики інформаційної безпеки клієнта;

b) функціювання процедур для періодичного зіставляння та перегляду відповідності певним законодавчим та регуляторним вимогам з інформаційної безпеки;

c) зміни у визначених заходах безпеки та як результат зміни в Положенні щодо застосовності;

d) впровадження та ефективність заходів безпеки згідно з програмою аудиту.

6.6.4 ОС повинен мати змогу до адаптації його програми наглядового аудиту з питаннями інформаційної безпеки, пов'язаними з ризиками та впливами на клієнта й підтвердити цю програму. Наглядові аудити можуть бути скомбіновані з аудитами інших систем управління. Звітування повинно чітко визначати аспекти, пов'язані з кожною системою управління.

Протягом наглядового аудиту ОС повинен перевірити записи апеляцій та скарг, які були подані раніше органу сертифікації на розгляд, а також перевірити, що там, де були виявлені будь-які невідповідності чи збої, які не відповідали вимогам сертифікації, клієнт дослідив свою власну СУІБ та процедури і виконав відповідні корегувальні дії.

Звіт щодо нагляду повинен містити зокрема інформацію стосовно усунення невідповідностей, які було виявлено раніше, і версію Положення щодо застосовності, а також важливі зміни після попереднього аудиту.

Щонайменше звіти після нагляду повинні бути сформовані так, щоб покривати в цілому вимоги наведені вище

6.7 Звіти про нагляд повинні містити відомості про усунення кожної невідповідності, що була виявлена раніше.

6.8 За результатами наглядового аудиту ОС може зупинити або скасувати дію сертифіката на систему управління у випадках:

• виявлення невідповідності системи управління якістю вимогам застосовного стандарту;

• підприємство не усунуло виявлені невідповідності протягом встановленого терміну;

• наявності обґрунтованих претензій споживачів даної продукції;

• виявлення порушень правил або процедур, установлених ОС;

• виявлення неправильного використання сертифіката.

6.9 ОС анулює сертифікат на систему управління у випадках:

• якщо результати наглядового аудиту свідчать про принципову невідповідність системи управління чинним вимогам;

• якщо виявлені при проведенні наглядового аудиту невідповідності не усунені протягом встановленого терміну;

• якщо протягом тривалого часу виробник не поставляє продукцію;

• якщо у разі зміни правил системи сертифікації виробник не може забезпечити відповідності новим вимогам;

• якщо виробник не виконав фінансові зобов'язані перед ОС;

• наявності офіційного прохання виробника.

6.10 Про тимчасове зупинення або скасування дії, про факт анулювання сертифіката ОС офіційно повідомляє підприємство.

6.11 Інші дії щодо наглядання можуть охоплювати: запити від ОС до сертифікованого замовника щодо аспектів сертифікації; аналізування будь-яких заяв сертифікованого замовника щодо його дій (наприклад, рекламних матеріалів, веб-сайту); запити сертифікованому замовнику щодо надання документів і записів (на паперових або електронних носіях); інші заходи моніторингу роботи сертифікованого замовника.

6.12 За результатами наглядового аудиту формується справа, яка зберігається в ОС та містить:

- завдання на проведення наглядового аудиту;
- план та графік аудиту;
- протоколи попередньої та заключної нарад;
- протоколи реєстрації невідповідностей (за наявності);
- звіт про наглядовий аудит;
- звіт від підприємства про усунення невідповідностей (при наявності невідповідностей);
- рішення;
- додаткову інформацію (за необхідності), надану підприємством.

7 СПЕЦІАЛЬНІ АУДИТИ

7.1 Розширення сфери сертифікації

7.1.1 Замовник подає до ОС заявку на переоформлення сертифікату на систему управління з вказанням причини переоформлення за встановленою ОС формою. До заявки необхідно надати комплект документів, який підтверджує відповідні зміни. ОС розглядає заявку і наданий комплект документів та готує рішення за заявкою, в якому визначаються дії щодо аудиту та рішення щодо можливості проведення робіт з розширення сфери сертифікації. Розширення сфери сертифікації може бути проведено у поєднанні з наглядовим аудитом. Рішення доводить до замовника.

7.1.2 У випадку, якщо клієнт сертифікований відповідно до вимог державного стандарту на систему управління (наприклад, за ДСТУ ISO 9001) і бажає отримати сертифікат на ту ж систему управління, але відповідно до вимог міжнародного стандарту (наприклад, ISO 9001), або навпаки, то клієнт подає до ОС заявку за встановленою формою (Ф-09.01-01). До заявки необхідно надати комплект документів, який підтверджує відповідні зміни в документації СУЯ клієнта. ОС розглядає заявку і наданий комплект документів та готує рішення за заявкою щодо можливості проведення робіт з розширення сфери. Розширення сфери здійснюється шляхом проведення наглядового аудиту.

7.2 Зміни вимог щодо сертифікації

7.2.1 При зміні вимог щодо сертифікації (зміни вимог стандарту, що застосовується введення нової версії застосовного стандарту, зміни вимог щодо проведення аудиту тощо) ОС зобов'язаний:

- повідомити сертифікованих клієнтів (які сертифіковані на відповідність вимогам застосовного стандарту) про відповідні зміни,
- повідомити сертифікованих клієнтів, що ОС має намір внести в документацію у відповідності з вимогами до сертифікації;
- взяти до уваги думки зацікавлених сторін, перш ніж виносити рішення про точну форму і дату надання чинності змінам;
- визначити реальні терміни, потрібні клієнту для внесення відповідних змін до системи управління (перехідний період);
- офіційно повідомити усіх сертифікованих клієнтів про нові вимоги і про необхідність здійснення належних заходів щодо їх урахування, та про тимчасову зупинку або анулювання сертифіката в разі їх невиконання в установлений термін.

7.2.2 Рішення щодо перехідного періоду приймається ОС на підставі рекомендацій відповідних національних чи міжнародних організацій.

7.2.3 Порядок та обсяг проведення робіт для перевірки виконання змінених вимог, ОС визначає в кожному конкретному випадку в залежності від обсягу та виду змін. Перевірка може бути проведена під час чергового/позапланового наглядового аудиту або процедура аналогічна процедурі сертифікації (згідно п.5 Порядку).

ОС ухвалює рішення щодо сертифікації чи переоформлення сертифікату (скасування чинного сертифікату та видачу нового сертифікату), ґрунтуючись на результатах перевірки виконання змінених вимог.

При проведенні перевірки виконання змінених вимог під час наглядового аудиту сертифікат видається після прийняття рішення щодо надання сертифікації на термін дії попереднього сертифікату.

7.3 Зміни в системі управління сертифікованого клієнта

7.3.1 Сертифікований клієнт зобов’язаний:

- оперативно інформувати ОС про будь-які передбачені зміни в системі управління або інші зміни, які можуть вплинути на її відповідність чинним вимогам;
- погодитися з рішенням ОС про необхідність переоцінки системи управління у зв’язку з включенням передбачених змін або здійснення додаткового аналізу цих змін.

7.4 Короткострокові аудити

7.4.1 ОС, в разі необхідності (щоб розслідувати скарги, або у відповідь на зміни, або щодо замовників, сертифікацію яких тимчасово зупинено), може провести аудит сертифікованих замовників попереджаючи незадовго до початку аудиту. В таких випадках, коли ОС прийняв рішення щодо проведення “особливого аудиту”, він письмово сповіщає сертифікованого замовника про умови проведення аудиту та склад групи аудиту. Оплата таких робіт здійснюється згідно з договором, який укладається між ОС та підприємством.

8 ПРИЗУПИНЕННЯ, СКАСУВАННЯ ТА СКОРОЧЕННЯ ГАЛУЗІ СЕРТИФІКАЦІЇ

8.1 ОС має право тимчасово зупинити дію сертифікатів у випадках, коли, наприклад:

− сертифікована система управління замовника постійно або суттєво не відповідає вимогам сертифікації, включаючи вимоги щодо результативності системи управління,

− сертифікований замовник не дозволяє проводити наглядові аудити або повторні сертифікаційні аудити з необхідною періодичністю, або

− сертифікований замовник добровільно подав прохання щодо призупинення.

8.2 За результатами наглядання ОС також може призупинити або скасувати дію сертифіката (п.6.4, п.6.5 даного порядку).

8.3 ОС укладаючи ліцензійну угоду з замовником на використання сертифікату відповідності, що має юридичну силу, інформує замовника про умови використання сертифікації, а також про дії замовника у разі призупинення чи скасування сертифікації.

8.4 Рішення про зупинку дії сертифікату відповідності та ліцензійної угоди приймається у випадку, якщо вжиттям коригувальних заходів, погоджених ОС, підприємство може усунути виявлені причини невідповідності. У протилежному разі сертифікат відповідності та ліцензійна угода скасовуються. Також сертифікат відповідності на систему управління скасовується у випадку розширення/скорочення сфери сертифікації і видачі нового сертифікату відповідності.

8.5 ОС повідомляє замовника аудиту та/або об'єкт аудиту про призупинку дії сертифіката листом і одночасно зазначає умови, за яких можливе поновити дію сертифіката на систему управління.

8.6 ОС призупиняє сертифікат на термін, що не перевищує 6 місяців від дати призупинки. Дію сертифіката відповідності може бути відновлено за умови виконання підприємством коригувальних заходів щодо усунення виявлених невідповідностей та позитивних результатів контролю їх виконання ОС, шляхом проведення наглядового аудиту. Якщо в зазначений термін замовник не виконує зазначених ОС умов, за яких можливе поновлення сертифікату на систему управління, ОС приймає рішення щодо анулювання сертифікату на систему управління.

8.7 Про факт анулювання сертифікату ОС офіційно повідомляє замовника аудиту листом або аналогічним повідомленням, направляється рішення щодо анулювання сертифікату (Ф-09.01-16).

8.8 ОС скорочує галузь сертифікації замовника, щоб виключити частки, які не відповідають вимогам, коли замовник постійно або серйозно не відповідає вимогам сертифікації відносно цих частин сфери сертифікації. Будь-яке таке скорочення повинне відповідати вимогам стандарту, що використовується для сертифікації.

9 ПОВТОРНЕ ОЦІНЮВАННЯ СИСТЕМИ УПРАВЛІННЯ

9.1 Термін дії сертифіката на систему управління не подовжується. Для отримання сертифіката на новий термін, підприємство за три місяці до закінчення терміну його дії подає до ОС заявку.

9.2 Проведення повторного оцінювання (ресертифікація) проводиться так само як і сертифікація системи управління. Порядок проведення повторної перевірки і оцінювання системи управління об'єкта аудиту визначає ОС в кожному конкретному випадку з урахуванням результатів наглядання за сертифікованою системою управління і наявності претензій та рекламацій до діяльності об'єкта аудиту. Діяльність з повторного сертифікаційного аудиту може не потребувати проведення аудит етапу 1. Рішення приймається ОС.

9.3 Ресертифікаційний аудит планується і проводиться для того, щоб оцінити постійне виконання всіх вимог використовуваного стандарту. Метою такого аудиту є підтвердження постійної відповідності і результативності системи управління в цілому, доречність і застосовність до сфери сертифікації.

9.4 При ресертифікаційному аудиті повинно враховуватися дієвість системи управління протягом періоду сертифікації і включати перевірку висновків попередніх наглядових аудитів.

9.5 При повторному оцінюванні група з аудиту може потребувати аудит етапу 1 аудиту, якщо відбулися суттєві зміни в системі управління, у замовника або в контексті функціонування системи управління (зміни в законодавстві).

9.6 При повторному оцінюванні розглядається:

- ефективність системи управління в цілому і стосовно внутрішніх і зовнішніх змін, постійної відповідності і придатності у сфері сертифікації;
- продемонстроване виконання зобов'язань підтримувати результативність і поліпшення системи управління для того, щоб удосконалювати усі показники;
- ефективність системи управління стосовно досягнення сертифікованим замовником цілей та запланованих результатів відповідної системи управління.

9.7 Якщо протягом ресертифікаційного аудиту виявлено невідповідності або відсутність доказів відповідності, ОС повинен визначити термін для розробки коригувальних дій, які повинні бути впроваджені підприємством до закінчення сертифікації.

9.8 ОС приймає рішення щодо ресертифікації на основі як результатів ресертифікаційного аудиту, так і на результатах аналізу системи управління протягом дії сертифікату та скарг, отриманих від користувачів сертифікації. Дата видання на новому сертифікаті повинна бути однаковою або пізнішою ніж дата рішення щодо повторної сертифікації.

9.9 Якщо ОС не завершив аудит повторної сертифікації або ОС не має можливості перевірити впровадження коригувань та коригувальних дій щодо будь-яких суттєвих невідповідностей до дати завершення сертифікації, повторна сертифікація не повинна бути рекомендована та дія сертифікації не повинна бути подовжена. Замовника потрібно поінформувати про таке рішення, а також про його наслідки.

Після закінчення дії сертифікації ОС може поновити сертифікацію в термін до 6 місяців за умови завершення всіх заходів з повторної сертифікації, в іншому випадку проводиться щонайменше аудит другого етапу. Дата набуття чинності сертифікатом повинна бути однаковою або пізнішою ніж дата рішення щодо повторної сертифікації. Дата завершення дії повинна ґрунтуватись на попередньому циклі сертифікації.

9.10 Організація здійснює оплату робіт з повторного оцінювання за окремим договором.

9.11 При внесенні змін до системи управління, яка була підтверджена під час сертифікації, замовник/об’єкт аудиту повинен оперативно інформувати ОС.

9.12 У разі наявності декількох ділянок або сертифікації на відповідність декільком стандартам системи управління, при плануванні аудиту повинен забезпечуватися відповідний обсяг аудиту на місці, щоб забезпечити довіру до сертифікації.

10 НЕПРАВИЛЬНЕ ВИКОРИСТАННЯ СЕРТИФІКАТА

10.1 Виробник не має права на використання сертифіката на систему управління у випадку:

- закінчення терміну дії, тимчасового зупинення дії або анулювання сертифіката;
- зміни виробником власної системи управління, яка не була прийнята ОС та, яка може негативно вплинути на відповідність вимогам системи управління;
- внесення ОС певних змін до правил системи, які виробник не зміг впровадити на своєму підприємстві;
- виникнення інших обставин, які можуть негативно вплинути на систему управління виробника.