Дана ВИПИСКА містить основні положення ПР-01 *СЕРТИФІКАЦІЯ СИСТЕМ УПРАВЛІННЯ*

*ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ*, що встановлює вимоги процесу сертифікації систем управління інформаційною безпекою, а саме:

**6. ЗАГАЛЬНІ ПОЛОЖЕННЯ**

6.1 Сертифікацію СУ проводять за ініціативою заявника, або за рішенням органу з сертифікації систем управління з метою підтвердження її відповідності вимогам ДСТУ ISO/IEC 27001:2015 і забезпечення впевненості в тому, що організація:

- здатна постійно надавати послуги, які задовольняють вимоги замовника та застосовні законодавчі і регламентувальні вимоги;

- своєчасно виявляє послугу незадовільної якості та вживає заходів щодо запобігання виробленню такої послуги на постійної основі;

- зорієнтована на підвищення задоволеності замовника завдяки результативному застосовування СУ, зокрема процесів поліпшування СУ та забезпечування відповідності вимогам замовника й застосовним законодавчим і регламентувальним вимогам.

Сертифікація СУ не підтверджує відповідність послуги вимогам.

Відповідальність за відповідність сертифікаційним вимогам несе організація, СУ якої сертифіковано.

6.2 Роботи з сертифікації СУІБ проводять відповідно до вимог
ДСТУ ISO/IEC 17021-1, ДСТУ ISO/IEC 27006, цієї СП, з урахуванням настанов, наведених у ДСТУ ISO 19011.

До проведення робіт із сертифікації СУІБ залучають підготовлений персонал, власний та залучений, та, за необхідністю, технічних експертів, власних та залучених.

Заявник визначає бажану сферу сертифікації. ОС визначає цілі аудиту та, за узгодженням із заявником, сферу та критерії аудиту. За результатами робіт із сертифікації ОС ухвалює рішення щодо сертифікації.

6.3 Цілі аудиту повинні визначати що має бути виконано при проведенні аудиту та включати:

- встановлення відповідності СУІБ, яка охоплює визначену заявником сферу сертифікації, критеріям аудиту;

- оцінку здатності СУІБ забезпечувати відповідність організації вимогам замовників та застосовним законодавчим і регламентувальним вимогам;

- оцінку результативності СУІБ стосовно забезпечення постійного досягнення організацією встановлених цілей у сфері якості.

6.4 Сфера аудиту повинна описувати обсяг та межі аудиту, враховуючи:

* місця розташування виробничих ділянок та структурних підрозділів організації;
* види діяльності та процеси, охоплені СУІБ;
* документацію СУІБ;
* термін проведення аудиту.

При проведенні аудиту ОС здійснює аналізування того чи охоплює СУІБ організації визначену заявником бажану сферу сертифікації.

6.5 Критерії аудиту повинні використовуватись як основа для визначення відповідності СУІБ, заявленої на сертифікацію, та включати вимоги, встановлені ДСТУ ISO/IEC 27001:2015 та документацією СУІБ заявника.

6.6 В ОС впроваджено в діяльність механізм дистанційної оцінки з врахуванням положень ДСТУ EN ISO/IEC 17021-1, IAF MD 4:2018 та IAF ID 12:2015 з використанням інформаційними та комунікаційними технологіями.

Дистанційна оцінка здійснюється згідно ***СП-13 «Порядок проведення діяльності дистанційно»*** та надає можливість підвищити оперативність проведення робіт з сертифікації СУ (оцінки), залучити персонал, який не може бути легко доступним, а також уникнути затримок та обмежень, що можуть виникнути під час поїздок з метою проведення оцінки на місці.

6.7 Вартість робіт, обсяги, терміни виконання, порядок оплати та відповідальність сторін визначаються договорами між заявником та ОС.

6.8 При проведенні робіт із сертифікації СУІБ ОС керується наступними принципами:

* неупередженість;
* компетентність;
* відповідальність;
* відкритість;
* конфіденційність;
* реагування на скарги;
* ризик-орієнтований підхід.

7. **ПРОЦЕС СЕРТИФІКАЦІЇ**

7.1. **Загальні положення**

Повний цикл сертифікації СУ складається з:

- первинної сертифікації, яка включає:

 - подання заявки на проведення сертифікації СУІБ та необхідної додаткової інформації (п.7.2.1 цієї СП);

 - аналізування заявки (п.7.2.2 цієї СП);

 - складання програми аудиту для повного циклу сертифікації (п.7.3.2 цієї СП);

 - укладання договору на проведення робіт із сертифікації СУІБ (п.7.3.3 цієї СП);

 - формування групи з аудиту (п.7.3.4 цієї СП);

 - первинний сертифікаційний аудит, який проводиться в два етапи:

 - перший етап аудиту (п.7.4.1 цієї СП);

 - другий етап аудиту (п.7.3.2 цієї СП);

- оформлення результатів та прийняття рішення щодо сертифікації
(п.7.3.3 цієї СП);

- наглядових аудитів за сертифікованою СУІБ протягом терміну дії сертифіката
(р.8 цієї СП);

- повторної сертифікації (р.9 цієї СП).

**7.2 Первинна сертифікація**

*7.2.1 Подання заявки на проведення сертифікації СУ та необхідної додаткової інформації*

Підставою для початку робіт із сертифікації СУ є подання заявником належним чином оформленої ***Заявки*** (Додаток 1) на проведення сертифікації СУ (далі - заявка).

Відповідальний виконавець ОС реєструє заявку в ***Журналі виконання робіт з сертифікації систем управління*** та направляє заявнику ***Опитувальну анкету*** (Додаток 2) і ***Перелік документів для проведення першого етапу аудиту*** (Додаток 3).

Рівень компетентності відповідального виконавця повинен бути достатнім для призначення його керівником групи з аудиту з урахуванням вимог ***СП-05 Управління персоналом, Р-01-ПР-01 Персонал органу з сертифікації. Порядок добирання та підготовки (стосовно систем управління якістю і/або інформаційною безпекою).***

Заявник заповнює опитувальну анкету та разом з визначеними документами подає до ОС.

Перед початком сертифікаційного аудиту ОС отримує від заявника відповідь на питання чи може бути недоступною для перегляду групою аудиту будь-яка пов’язана із СУІБ інформація (така, як записи СУІБ або інформація стосовно побудови та ефективності заходів безпеки), оскільки вона містить конфіденційну або чутливу інформацію. На основі отриманої інформації ОС визначає, чи можна адекватно здійснити аудит СУІБ без такої інформації. Якщо ОС надійшов висновку, що нема можливості адекватно здійснити аудит СУІБ без перегляду ідентифікованої конфіденційної або чутливої інформації, він повинен повідомити заявника, що сертифікаційний аудит не може бути здійсненим, доки відповідні угоди про надання доступу не буде підписано.

Інформація, що надана заявником, повинна містити наступну інформацію стосовно організації, СУ якої заявлена на сертифікацію:

- бажану сферу сертифікації;

- назву, юридичну адресу, адресу(и) фактичного місцезнаходження, суттєві аспекти процесів та операцій, будь-які доречні зобов’язання згідно діючого законодавства;

- загальну інформацію відносно бажаної сфери сертифікації, таку як види діяльності, людські та технічні ресурси, функції та взаємозв’язки в рамках корпорації, за наявності;

- інформацію стосовно всіх процесів, які використовуються організацією на умовах аутсорсингу та можуть впливати на відповідність вимогам;

- інформацію щодо отримання консультування стосовно СУІБ.

***Примітка.*** *Заявник несе повну відповідальність за достовірність і повноту інформації, що подається до ОС*.

У разі відмови заявника (в усній або письмовій формі) від проведення або оплати робіт із сертифікації після реєстрації заявки в ОС, відповідальний виконавець анулює заявку та вносить інформацію про її анулювання в ***Журнал робіт із сертифікації систем управління.***

*7.2.2 Аналізування заявки*

Відповідальний виконавець аналізує надані заявку та документи з метою забезпечення впевненості в наступних фактах:

* інформація про організацію та впроваджену в ній СУ є достатньою для розробки програми аудиту;
* будь-які відомі непорозуміння між органом з сертифікації та організацією вирішені;
* орган з сертифікації має компетентність і спроможність виконувати сертифікаційну діяльність;
* бажана сфера сертифікації, місцезнаходження виробничих ділянок організації, необхідна тривалість для проведення аудиту і будь-які інші питання, що впливають на процес сертифікації, були враховані (мова, умови безпеки, загрози неупередженості тощо).

За результатами аналізування заявки відповідальний виконавець оформлює ***Рішення за результатами аналізування заявки*** (Додаток 4) та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). У будь – якому випадку рішення приймає особа, яка не брала участі в проведенні аудиту. Рішення оформлюється в двох примірниках: один зберігається в ОС, другий направляється заявнику.

У разі позитивного рішення ОС продовжує роботи з сертифікації.

У разі негативного рішення роботи за заявкою припиняються. Негативне рішення має бути обґрунтоване з метою забезпечення відсутності конфлікту з принципами, зазначеними в
п. 6.8 цієї СП.

*7.2.5 Складання програми аудиту для повного циклу сертифікації*

За позитивних результатів аналізування заявки, з метою визначення діяльності з аудиту, яка повинна продемонструвати, що СУІБ заявника відповідає вимогам сертифікації, відповідальний виконавець розробляє ***Програму аудиту для повного циклу сертифікації*** (Додаток 5), яка повинна визначати два етапи первинного аудиту, наглядові аудити в першому і другому році після прийняття рішення про сертифікацію та аудит повторної сертифікації на третій рік до закінчення сертифікації. Перший трирічний цикл сертифікації починається з рішення щодо сертифікації. Подальші цикли починаються з рішення щодо повторної сертифікації. Визначення програми та будь-які подальші коригування повинні враховувати:

- розмір організації;

- сферу застосування та складність СУІБ та її процесів;

- продемонстрований рівень результативності СУІБ;

- результати попередніх аудитів.

Група аудиторів вимагати, щоб заявник виконав усі необхідні погодження для доступу до звітів внутрішніх аудитів і звітів з незалежного перегляду інформаційної безпеки.

Заявником повинна бути надана принаймні така інформація протягом стадії 1 сертифікаційного аудиту:

a) загальна інформація стосовно СУІБ і діяльності, яку вона охоплює;

b) копії потрібної документації СУІБ, визначеної в ISO/IEC 27001 і, де потрібно, пов’язаної з нею

документації.

ОС не здійснює сертифікацію СУІБ, доки вона не пройшла хоча б оди перегляд з боку керівництва та один внутрішній аудит СУІБ, що покриває сферу застосування сертифікації.

Програма оформлюється в двох примірниках (один примірник зберігається в ОС, другий направляється заявнику), підписується відповідальним виконавцем та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). З програмою, до укладення договору на проведення робіт із сертифікації СУ, необхідно ознайомити керівника (відповідальну особу) організації з метою вирішення можливих спірних питань щодо її змісту.

7.2.2 *Визначення тривалості аудиту*

Розрахунок тривалості аудиту СУІБ здійснюється з урахуванням вимог ***РІ-03 Розрахунок тривалості аудиту*** та ***ДСТУ ISO/IEC 27006:2015,п.9.1.4 та Додаток В, Додаток С.***

***7.2.3 Використання вибірки при розгалуженій структурі.***

Коли заявник має розгалужену структуру представництв, які відповідають критеріям від a) до c), наведеним нижче, орган сертифікації може розглянути вибірковий підхід сертифікаційного аудиту розгалуженої мережі представництв:

a) усі представництва функціонують у рамках однієї СУІБ, для якої забезпечено централізоване адміністрування та аудит, і вони є суб’єктом перегляду центрального керівництва;

b) усі представництва долучені до програми внутрішнього аудиту СУІБ заявника;

c) усі представництва долучені до програми перегляду СУІБ з боку керівництва заявника.

При застосуванні вибіркового підходу головний аудитор враховує наступні вимоги:

a) при укладанні договору на сертифікацію з організацією-замовником виявляється, наскільки це можливо, різниця між об'єктами (площадками), щоб можна було визначити адекватний рівень вибірки;

b) пепрезентативну кількість представництв визначається ОС з урахуванням:

1) результатів внутрішніх аудитів головного офісу та представництв;

2) результатів переглядів з боку керівництва;

3) варіантів розмірів представництв;

4) варіантів в бізнес-цілях представництв;

5) складності інформаційних систем у різних представництвах;

6) варіантів у робочих практиках;

7) варіантів у виконуваних діях;

8) варіантів побудови та функціювання заходів безпеки;

9) потенційної взаємодії з критичними інформаційними системами або інформаційними сис-

темами, які обробляють чутливу інформацію;

10) будь-яких законодавчих вимог, що відрізняються;

11) географічних та культурних аспектів;

12) ситуацій з ризиками в представництвах;

13) інцидентів інформаційної безпеки в специфічних представництвах.

c) репрезентативна вибірка складається з усіх представництв у межах сфери застосування СУІБ організації; цей вибір повинен базуватися на критичному виборі для відображення чинників, які надано в b) вище, а також випадковому елементі.

d) для кожного представництва, охопленого СУІБ, яке є суб’єктом значних ризиків, здійснює аудит ОС перед сертифікацією.

e) програма аудиту розробляється з урахуванням наведених вище вимог, а також повинна покривати

репрезентативну вибірку в межах сфери застосування сертифікації СУІБ у рамках періоду в три роки.

f) якщо було виявлено невідповідність або в головному офісі, або в окремому представництві, процедуру коригувальних дій застосовують до головного офісу та всіх представництв, які покриваються сертифікатом.

Аудит повинен показати, що дії в головному офісі організації заявника гарантують, що єдину СУІБ застосовують для всіх представництв і доводить центральне управління на операційний рівень. Аудит повинен розглядати всі питання, зазначені вище.

Обгрунтування плану вибірки документується в ***Програмі аудиту.***

*7.2.4 Множина систем управління*

*Інтеграція документації СУІБ з документацією інших систем управління*

ОС може приймати документацію, яка є комбінованою (наприклад, для інформаційної безпеки, якості, охорони здоров’я та безпеки й навколишнього середовища), а також СУІБ може бути чітко ідентифікована разом із відповідними інтерфейсами до інших систем.

*Комбіновані аудити систем управління*

Аудит СУІБ може бути скомбінованим з аудитами інших систем управління за умови, що він може

продемонструвати, що такий аудит відповідає всім вимогам для сертифікації СУІБ. Усі елементи, важ-

ливі для СУІБ, повинні бути чітко та без зусиль ідентифіковані у звітах аудиту. На якість аудиту не по-

винна впливати комбінація аудитів.

*7.2.6. Укладення договору на проведення робіт із сертифікації СУ*

Усі роботи з сертифікації СУІБ оплачуються заявником на підставі договору, що укладається з ТОВ «ІМПЕРІУМ СЕРТИФІК». Якщо при виконанні робіт, на будь – якому етапі виникне недоцільність їх продовження, ОС повертає заявнику суму вартостей робіт, які не виконуватимуться.

Договір підписується керівником ТОВ «ІМПЕРІУМ СЕРТИФІК (особою, якій делеговане право на виконання цих функцій) та заявником.

*7.2.7. Формування групи з аудиту*

Якщо ОС не приймає іншого рішення, функції керівника групи з аудиту виконує відповідальний виконавець, який, з урахуванням результатів аналізування заявки, встановлює рівень компетентності, необхідний для проведення робіт із сертифікації СУ, та надає пропозиції стосовно членів групи з аудиту шляхом оформлення в двох примірниках проекту ***Складу групи з аудиту*** (Додаток 6), який візується виконавцем та надається для затвердження керівнику ОС (особі, якій делеговане право на виконання цих функцій). Затверджений склад групи з аудиту завчасно направляється заявнику для ознайомлення під підпис. Заявник може заперечити щодо включення до групи з аудиту будь-яких аудиторів чи технічних експертів за наявності об’єктивних причин (наприклад, якщо член групи мав у минулому, або має з організацією взаємозв’язки, які можуть нести загрозу неупередженості, відзначився неетичною поведінкою в минулому тощо) шляхом направлення ОС офіційного листа. За умови підтвердження об’єктивності заперечень заявника, ОС вносить зміни до складу групи з аудиту, про що в зазначеному вище порядку повідомляє заявника. За відсутності об’єктивних причин для заперечень, ОС не змінює склад групи з аудиту, про що повідомляє заявника офіційним листом.

З урахуванням затвердженого складу групи з аудиту відповідальний виконавець оформлює за встановленою формою проект наказу (розпорядження), який візується виконавцем та надається для затвердження керівнику ОС (особі, якій делеговане право на виконання цих функцій).

При визначенні розміру та складу групи з аудиту враховуються:

* цілі аудиту, сфера, критерії та розрахункова тривалість аудиту;
* чи є аудит комплексним, інтегрованим або спільним;
* загальна компетентність групи з аудиту для досягнення цілей аудиту;
* сертифікаційні вимоги (включаючи застосовні законодавчі, регуляторні та договірні вимоги);
* мова та культура.

Необхідний рівень компетентності повинен бути у всієї групи в цілому, а не у кожного окремого члена групи. За необхідності до складу групи з аудиту можуть бути включені технічні експерти, письмові та усні перекладачі, які повинні працювати під керівництвом аудитора.

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 заявник 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 заявника.

Якщо в групі з аудиту є тільки один аудитор, він повинен мати компетентність для виконання обов’язків керівника групи з аудиту.

Вимоги до критеріїв компетентності персоналу, який залучається до проведення робіт із сертифікації встановлені в ***СП-05 Управління персоналом***, ***РІ-03-ПР-03 Персонал органу з сертифікації систем управління.  Порядок добирання та підготовки***

(стосовно систем управління інформаційною безпекою)

До складу групи з аудиту не можуть бути включені представники заявника, організації, де проводиться аудит, та організацій, зацікавлених в результатах сертифікації.

До складу групи з аудиту можуть бути включені аудитори - стажисти, за умови, що один із аудиторів буде призначений оцінювачем їх діяльності. Оцінювач повинен бути достатньо компетентним для виконання обов’язків та нести остаточну відповідальність за діяльність та висновки аудиторів-стажистів.

Керівник групи з аудиту, за узгодженням із членами групи з аудиту, розподіляє обов’язки стосовно проведення аудиту конкретних процесів, функцій, об’єктів, галузей або діяльності, охоплених СУ, враховуючи при цьому необхідну компетентність, результативність та ефективність використання можливостей групи з аудиту, а також різні функції та обов'язки аудиторів, аудиторів-стажистів і технічних експертів. Для досягнення цілей аудиту, під час проведення аудиту керівник групи з аудиту може вносити зміни до розподілу обов’язків.

При проведенні аудиту, за узгодженням між ОС та заявником, можуть бути присутні спостерігачі (наприклад, члени організації, в якій проходить аудит, консультанти, персонал органу з акредитації, представники регулятивних органів, інші особи, за наявності обґрунтування) та/чи супроводжуючі (особи, які призначаються з метою сприяння членам групи з аудиту в проведенні аудиту). Група з аудиту повинна забезпечити відсутність впливу спостерігачів та супроводжуючих на процес чи результати аудиту.

*7.2.6 Первинний сертифікаційний аудит*

Первинний сертифікаційний аудит СУ проводиться в два етапи: перший етап аудиту та другий етап аудиту.

Перший та другий етапи аудиту проводяться групою з аудиту, сформованою згідно з
п. 7.2.5 цієї СП. Наказ (розпорядження) про призначення групи з аудиту може оформлюватись для кожного етапу аудиту окремо, або для обох етапів аудиту разом. У будь – якому випадку до складу групи з аудиту для проведення другого етапу аудиту обов’язково включаються члени групи з аудиту, які проводили перший етап аудиту.

**7.3.1 Перший етап аудиту**

Для проведення першого етапу аудиту група з аудиту під керівництвом керівника групи розробляє ***Програму першого етапу аудиту*** (Додаток 7) ***.***

***План аудиту*** СУІБ повинен враховувати визначені заходи інформаційної безпеки.

В ***План аудиту*** ідентифікують методики здійснення аудиту з використанням мережі, які будуть застосовувати протягом аудиту, якщо це застосовно. Методики аудиту з використанням мережі можуть включати, наприклад, телеконференції, webзустрічі, інтерактивні, основані на web-технологіях комунікації та віддалений електронний доступ до документації СУІБ чи процесів СУІБ. Ціллю таких методик є підвищення ефективності та продуктивності аудиту, а також підтримування цілісності процесу аудиту.

Часовий розклад аудиту, який буде найкращим чином демонструвати повну сферу застосування аудиту організації, розробляється ОС та погоджується з організацією, яка підлягає аудиту. Розгляд може включати сезони, місяці, дні/дати й перенесення, якщо це застосовно.

***Програма першого етапу аудиту та План аудиту*** (Додаток 7)оформлюється в двох примірниках, підписується членами та керівником групи з аудиту та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). Один примірник програми зберігається в ОС, другий направляється заявнику.

Перший етап аудиту проводиться з метою:

* перевірити задокументовану інформацію системи СУІБ організації;
* отримати достатнє розуміння побудови СУІБ з урахуванням обставин організації заявника;
* оцінити конкретний стан ділянки організації та провести співбесіди з персоналом організації з метою визначення готовності до другого етапу аудиту;
* проаналізувати стан організації та його розуміння щодо вимог ДСТУ ISO/IEC 27001, зокрема стосовно визначення ключових характеристик або суттєвих аспектів, процесів, цілей і функціювання СУІБ;
* зібрати необхідну інформацію щодо сфери СУІБ, включаючи:
* ділянки;
* процеси та обладнання;
* оцінювання та оброблення ризиків (зокрема й визначені заходи безпеки);
* встановлені рівні контролю (зокрема у випадках організацій з розгалуженою структурою);
* застосовні законодавчі та регуляторні вимоги;
* проаналізувати розподіл ресурсів для проведення аудиту другого етапу і погодити з організацією деталі аудиту другого етапу;
* забезпечити конкретизацію планування аудиту другого етапу завдяки досягненню достатнього розуміння СУІБ організації і діяльності її дільниць в контексті ДСТУ ISO/IEC 27001 або інших нормативних документів;
* оцінити, чи планують і провадять внутрішні аудити і аналізування з боку керівництва, і чи ступень запровадження СУІБ підтверджує готовність організації для аудиту другого етапу.

У разі необхідності керівник групи з аудиту може направити члена групи в організацію з метою проведення першого етапу аудиту на місці, або запросити від заявника додаткову інформацію.

Одночасно з аналізуванням інформації, отриманої від заявника, група з аудиту може організувати збір від незалежних джерел та аналізування додаткових відомостей, пов’язаних, наприклад, із виконанням організацією встановлених вимог щодо якості та безпечності послуг.

За результатами проведення першого етапу аудиту група з аудиту під керівництвом керівника групи оформлює ***Висновок за результатами проведення першого етапу аудиту*** (Додаток 8), який містить:

- узагальнені результати першого етапу аудиту;

- проблемні питання, що можуть бути класифіковані як невідповідності під час проведення другого етапу аудиту (за наявності);

- невідповідності (за наявності);

- висновок щодо доцільності (недоцільності) проведення другого етапу аудиту.

Висновок оформлюється в двох примірниках, підписується членами та керівником групи з аудиту та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). Один примірник висновку зберігається в ОС, другий направляється заявнику.

Термін підготовки висновку не повинен перевищувати 1 місяця з дати закінчення проведення першого етапу аудиту. За наявності обґрунтованих причин висновок може бути підготовлений у термін, що перевищує зазначений термін, з обов’язковим повідомленням про це заявника.

ОС, в особі керівника ОС (особи, якій делеговане право на виконання його функцій), на підставі оцінки інформації, наведеної в висновку за результатами проведення першого етапу аудиту, та будь – якої іншої інформації (наприклад, загальнодоступна інформація, коментарі від заявника) приймає і документує ***Рішення щодо доцільності (недоцільності) проведення другого етапу аудиту*** (Додаток 9). Проект рішення візується виконавцем та підписується керівником ОС (особою, якій делеговане право на виконання цих функцій). У будь – якому випадку рішення приймає особа, яка не брала участі в проведенні аудиту. Рішення оформлюється в двох примірниках: один зберігається в ОС, другий направляється заявнику.

***Примітка 1.*** *У випадку виявлення в процесі проведення першого етапу аудиту даних, що можуть бути класифіковані як невідповідності під час проведення другого етапу аудиту, чи невідповідностей, які можуть бути усунені організацією в термін до шести місяців, приймається рішення щодо доцільності проведення другого етапу аудиту. ОС при цьому планує заходи з проведення другого етапу аудиту з урахуванням терміну, необхідного організації для вирішення проблемних питань, результативність вирішення яких перевіряється при проведенні другого етапу аудиту.*

***Примітка 2.*** *У випадку виявлення в процесі проведення першого етапу аудиту суттєвих невідповідностей, які можуть бути усунені організацією лише протягом тривалого часу (більше шести місяців), приймається рішення щодо недоцільності проведення другого етапу аудиту. Подальші роботи з сертифікації не проводяться. Після усунення всіх невідповідностей організація має право повторно подати заявку на проведення сертифікації СУ згідно з п. 7.2.1 цієї СП.*

**7.3.2 Другий етап аудиту**

*7.3.2.1 Загальні положення*

Другий етап аудиту проводиться безпосередньо на місці (місцях) розташування організації з метою оцінки впровадження СУІБ та отримання підтвердження, що заявник дотримується своїх власник політик, цілей і процедур та концентрується на:

* інформації та доказах відповідності всім вимогам ДСТУ ISO/IEC 27001 або інших нормативних документів;
* відповідність СУІБ та діяльності організації застосовним законодавчим, регуляторним та договірним вимогам;
* провідній ролі та зобов’язаннях вищого керівництва організації заявника стосовно політики інформаційної безпеки та цілей інформаційної безпеки;
* вимогах документації, зазначених в ISO/IEC 27001;
* оцінюванні ризиків, пов’язаних з інформаційною безпекою, і тому, що оцінювання призводить до постійних, цінних і порівняних результатів, якщо його виконують повторно;
* визначенні цілей заходів безпеки та заходів безпеки, основаних на оцінці ризиків інформаційної безпеки та процесів оброблення ризиків;
* результативності інформаційної безпеки та ефективності СУІБ у разі зіставляння з цілями інформаційної безпеки;
* відповідності між визначеними заходами безпеки, Положенням щодо застосовності та результатами оцінки ризиків інформаційної безпеки і процесу оброблення ризиків та політики і цілей інформаційної безпеки;
* впровадженні заходів безпеки (з урахуванням настанов, описаних в Додатку D ДСТУ ISO/IEC 27006:2015) 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;
* 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.

 Аудити «на місці» можуть включати дистанційний доступ до електронної(них) ділянки(нок), що містить(тять) інформацію, яка відноситься до аудиту СУІБ. В цьому випадку використовуються електронні засоби для проведення аудитів.

*7.3.2.2 Розробка програми другого етапу аудиту та плану аудиту*

На підставі результатів проведення першого етапу аудиту група з аудиту під керівництвом керівника групи розробляє ***Програму другого етапу аудиту*** (Додаток 10) та ***План аудиту*** (Додаток 11). ***Програма другого етапу аудиту*** підписується керівником і всіма членами групи з аудиту та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). План аудиту підписується керівником групи з аудиту.

З програмою другого етапу аудиту та планом аудиту до початку проведення другого етапу аудиту необхідно ознайомити керівника (відповідальну особу) організації з метою вирішення можливих спірних питань щодо змісту програми та/чи плану. Спірні питання мають бути вирішені між керівником групи з аудиту та керівником (відповідальною особою) організації. В ході аудиту керівник групи з аудиту має право, за узгодженням із керівником (відповідальною особою) організації, вносити зміни в план аудиту.

У разі, якщо ділянки організації, на яких здійснюється аналогічна діяльність, охоплена СУ, розташовані в різних місцях, ОС може здійснювати вибіркові перевірки цих ділянок. Для забезпечення проведення належного аудиту програма другого етапу аудиту та план аудиту в такому випадку розробляються з урахуванням вибірки, яка повинна бути обґрунтованою.

Програма другого етапу аудиту та план аудиту в загальному випадку мають містити інформацію про:

- цілі аудиту;

- сферу аудиту;

- критерії аудиту;

- підстави для проведення аудиту;

- склад групи з аудиту;

- дату проведення аудиту;

- розподіл обов’язків між членами групи з аудиту;

- джерела інформації про якість послуги;

- обґрунтування вибірки (у разі застосування);

- очікуваний час тривалості аудиту;

- спостерігачів та супроводжувачів;

- вимоги щодо забезпечення конфіденційності інформації;

- перелік організацій та осіб, яким надається звіт про перевірку.

У разі необхідності члени групи з аудиту розробляють форми робочих документів (переліки контрольних питань, форми для реєстрації спостережень, форми для документування допоміжних даних та ін.). Робочі документи повинні бути такими, щоб не обмежувати проведення додаткових заходів, необхідність в яких може бути виявлена в процесі проведення аудиту.

*7.3.2.3 Проведення другого етапу аудиту*

Другий етап аудиту включає:

* проведення попередньої (вступної) наради;
* проведення обстеження шляхом збирання та перевіряння інформації;
* підготування висновків аудиту та проведення заключної наради;
* оформлення результатів перевірки.

*7.3.2.4 Проведення вступної наради*

Вступну нараду організовують та проводять організація та керівник групи з аудиту. У нараді беруть участь члени групи з аудиту та персонал організації, який призначено для участі в проведенні аудиту. Попередня нарада проводиться з метою:

- представлення членів групи з аудиту та їхніх функцій;

- підтвердження бажаної сфери сертифікації;

- підтвердження програми та плану аудиту (зокрема, типу аудиту, сфери, цілей і критеріїв аудиту);

- узгодження дати й часу проведення заключної наради та проміжних нарад (за необхідності);

- встановлення офіційних способів спілкування між групою з аудиту та персоналом організації;

- підтвердження забезпеченості групи з аудиту необхідними ресурсами;

- підтвердження положень щодо конфіденційності інформації;

- підтвердження відповідних процедур для групи з аудиту, пов’язаних з охороною праці, надзвичайними ситуаціями та безпекою;

- підтвердження наявності та функцій супроводжувачів та спостерігачів;

- порядок звітування, включаючи класифікацію даних аудиту;

- інформування про умови, за яких аудит може бути достроково припинено;

- підтвердження того, що група з аудиту несе відповідальність за аудит і буде контролювати виконання плану аудиту;

- підтвердження статусу даних за результатами попередніх аналізувань або аудитів, за наявності;

- підтвердження методів і процедур, які будуть використовуватись для проведення аудиту на основі вибірки;

- підтвердження мови, яка буде використовуватись в ході аудиту;

- підтвердження того, що під час аудиту організація буде отримувати інформацію про хід аудиту та будь-які проблемні питання;

- з’ясування незрозумілих питань.

За результатами вступної наради керівником групи з аудиту складається та підписується ***Протокол вступної наради*** (Додаток 12) та, за необхідності, вносяться зміни в план аудиту, зокрема в розподіл обов’язків між аудиторами.

***Протокол вступної наради*** оформлюється в двох примірниках: один зберігається в ОС, інший надається заявнику.

*7.3.2.5 Обмін інформацією при проведенні аудиту*

При проведенні аудиту члени групи з аудиту періодично оцінюють отримані дані аудиту та обмінюються інформацією. Керівник групи з аудиту, за необхідності, перерозподіляє обов’язки між членами групи з аудиту та періодично інформує заявника про досягнуті результати та будь-які проблемні питання.

Якщо отримані дані аудиту свідчать про недосяжність цілей аудиту, або передбачають наявність безпосереднього суттєвого ризику (наприклад, загрозу безпеці), керівник групи з аудиту повідомляє про це заявника та, за можливості, ОС, з метою прийняття рішення щодо подальших дій. Такі дії можуть включати повторне підтвердження або внесення змін до плану аудиту, цілей аудиту, сфери аудиту, або припинення аудиту. Керівник групи з аудиту повідомляє керівнику ОС про результати застосованих дій.

Керівник групи з аудиту разом з заявником аналізує будь-яку необхідність внесення змін до сфери аудиту, яка стає очевидною в ході проведення аудиту, та повідомляє про це керівнику ОС.

*7.3.2.6 Збирання та перевіряння інформації при проведенні аудиту*

Для одержання доказів аудиту та оцінки здатності організації забезпечувати інформаційну безпеку, яка відповідає встановленим вимогам, група з аудиту, на підставі відповідних вибіркових методів, збирає та перевіряє інформацію, що стосується цілей, сфери та критеріїв аудиту, включаючи інформацію щодо взаємозв’язків між функціями, діяльністю та процесами, охопленими СУ. Інформацію збирають шляхом співбесід, аналізування документації, здійснення спостережень за процесами та діяльністю.

При проведенні аудиту СУІБ група аудиторів повинна:

- вимагати, щоб заявник продемонстрував, що оцінка ризиків, пов’язаних з інформаційною безпекою, є доречною та адекватною для операцій СУІБ у межах сфери застосування СУІБ;

- визначити, чи процедури заявника для ідентифікації, перевірки та оцінювання ризиків, пов’язаних з інформаційною безпекою, та результати їх впровадження відповідають політиці, цілям і намірам заявника.

В ході аудиту СУІБ ОС встановлює, чи процедури, застосовані в оцінці ризиків, є належними і відповідним чином впроваджені.

*7.3.2.7 Ідентифікація та реєстрування даних аудиту*

Для підготування даних аудиту, узагальнюючих відповідності та деталізуючих невідповідності, докази аудиту оцінюють за критеріями аудиту. Дані аудиту та їх підтверджувальні докази повинні реєструватись.

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

Невідповідності та спостереження, виявлені при проведенні аудиту, та докази, які їх підтверджують, повинні реєструватись у ***Протоколах невідповідностей/спостережень*** (Додаток 13) з посиланням на конкретні вимоги критеріїв аудиту. Невідповідності класифікують, як суттєві і несуттєві. З метою підтвердження точності одержаних доказів аудиту та забезпечення правильного розуміння невідповідностей, група з аудиту обговорює невідповідності з організацією, реєструючи в протоколах невідповідностей усі розбіжності. Організація аналізує виявлені невідповідності, та їх причини та зазначає в протоколах невідповідностей причини невідповідностей, зміст необхідних коригувань, коригувальних дій та терміни їх впровадження. Група з аудиту аналізує коригування, визначені причини і коригувальні дії з метою визначення їх прийнятності.

Докази, що підтверджують усунення невідповідності повинні бути зареєстровані. Організацію потрібно проінформувати щодо результатів аналізування та перевіряння та, у разі потреби в додатковому повному або скороченому аудиті або щодо надання задокументованих доказів (що будуть підтверджені під час майбутніх аудитів) для перевірки результативності коригувань та коригувальних дій.

Група з аудиту перевіряє результативність будь-яких запроваджених коригувань та коригувальних дій. Перевіряння результативності коригування та коригувальної дії може бути здійснено на основі аналізування документації, наданої організацією, або, у випадку необхідності, шляхом перевіряння на місці.

*7.3.2.8 Підготування висновків аудиту. Проведення заключної наради*

Перед заключною нарадою, група з аудиту:

- аналізує дані аудиту та будь-яку іншу відповідну інформацію, отримані при проведенні першого та другого етапів аудиту, відносно цілей аудиту;

- узгоджує висновки аудиту, з урахуванням невизначеності, яка властива процесу аудиту;

- визначає будь-які необхідні подальші дії;

- підтверджує відповідність програми та плану аудиту або визначає будь-які необхідні зміни (наприклад, щодо сфери аудиту, тривалості або термінів проведення аудиту, періодичності наглядових аудитів, компетентності).

Офіційна заключна нарада проводиться керівником групи з аудиту, в присутності членів групи з аудиту, керівництва організації та, за необхідності, осіб, відповідальних за перевірені функції або процеси.

Мета заключної наради - надати керівництву організації висновки аудиту та попередні висновки щодо можливості (неможливості) видачі сертифіката на систему управління інформаційною безпекою організації. Будь – які невідповідності повинні бути представлені залежно від їх вагомості таким чином, щоб вони були зрозумілими, а терміни для реагування на них були узгоджені.

На заключній нараді, в загальному випадку, розглядають також наступні питання:

* доведення до відома заявника того, що зібрані докази аудиту були засновані на вибірковій інформації, що тим самим спричиняє елемент невизначеності;
* спосіб та терміни звітування;
* процес розгляду невідповідностей органом із сертифікації, зокрема, будь-які наслідки, пов'язані із сертифікаційним статусом заявника;
* необхідність здійснення організацією аналізування причин виявлених невідповідностей та надання плану коригувань та коригувальних дій протягом встановленого терміну;
* застосовні дії ОС після проведення аудиту;
* інформація щодо процесів розгляду скарг та апеляцій.

Між групою з аудиту та організацією обговорюються будь-які суперечності щодо даних аудиту та висновків аудиту. Всі невирішені суперечності реєструються в протоколі заключної наради та повідомляються ОС.

За результатами проведення наради оформлюється ***Протокол заключної наради*** (Додаток 14), який підписують усі члени групи з аудиту. З протоколом під підпис ознайомлюється керівник (уповноважена особа) організації. Протокол заключної наради оформлюється в двох примірниках: один зберігається в ОС, інший надається заявнику.

**7.3.3 Оформлення результатів**

*7.3.3.1 Звіт про перевірку*

За результатами проведення аудиту СУІБ група з аудиту під керівництвом керівника групи оформлює ***Звіт про перевірку*** СУІБ (далі - звіт) (Додаток 15). При цьому кожний член групи з аудиту надає інформацію для звіту стосовно тих елементів СУ, аудит яких він здійснював відповідно до плану аудиту. Керівник групи з аудиту несе відповідальність за повноту та достовірність звіту. Звіт повинен містити достовірний, стислий і чіткий опис проведеного аудиту, включаючи, або посилаючись на:

- загальну інформацію про організацію, в якій проводився аудит (назву, адресу, банківські реквізити, представника організації), та про ОС (назву, адресу, банківські реквізити, реєстраційний номер свідоцтва про призначення та/чи атестата про акредитацію);

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

* інформацію про підстави для проведення аудиту;

- цілі, критерії аудиту, сферу аудиту;

- інформацію про склад групи з аудиту та супроводжуючих осіб;

- інформацію про технічних експертів (у разі їх залучення);

- інформацію про терміни та місця проведення аудиту;

- результати першого етапу аудиту та висновок за ними;

- відомості про програму другого етапу аудиту та план аудиту;

* будь-які відхилення від плану аудиту та їх причини;
* будь-які значні питання, що впливають на програму аудиту;
* значні зміни, якщо такі є, що негативно вплинули на СУІБ організації з часу проведення останнього аудиту;

- дані аудиту;

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

- дані щодо невідповідностей та, у разі застосування, щодо коригувань і коригувальних дій, вжитих організацією;

- підтвердження інформації, наданої ОС при аналізуванні заявки (п. 4.2.2 цієї СП);

- будь-які невирішені суперечності, за наявності;

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

- висновки аудиту;

- рекомендацію від групи з аудиту щодо можливості (неможливості) видачі сертифіката разом з будь – якими умовами та зауваженнями;

* результативність, з якою організація заявника, аудит якої було проведено, контролює використання документів про сертифікацію та знаків, якщо це застосовно;
* перевірка результативності запроваджених коригувальних дій стосовно невідповідностей, встановлених раніше, якщо це застосовно;

- вказівку про конфіденційність інформації, наведену в звіті;

- відомості щодо організацій та осіб, яким надається звіт.

* заяву про відповідність та результативність СУІБ разом з підсумком доказів, що відносяться до:

 -можливості СУІБ 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.

Звіт повинен також містити:

- змістовний журнал аудиту і застосовану методику аудиту;

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

- коментарі стосовно відповідності СУІБ заявника 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 заявника.

Рекомендація щодо можливості (неможливості) видачі сертифіката повинна ґрунтуватися на одному з наступних висновків:

1. СУ результативна та повністю відповідає вимогам ДСТУ ISO/IEC 27001:2015;
2. СУ результативна та в цілому відповідає вимогам ДСТУ ISO/IEC 27001:2015, але виявлено невідповідності, які можуть бути усунені в термін до 6 місяців;
3. СУ не результативна та/або має невідповідності, які можна усунути лише в результаті доопрацювання в термін понад 6 місяців.

Звіт підписують члени та керівник групи з аудиту та затверджує керівник ОС (особа, якій делеговане право на виконання цих функцій). Зі звітом під підпис ознайомлюється керівник (уповноважений представник) організації, в якій проводився аудит. Один примірник звіту направляється в ОС, два примірники – заявнику. За узгодженням між ОС та заявником, можуть бути оформлені та направлені будь-яким організаціям та особам додаткові примірники звіту.

Термін підготовки звіту не повинен перевищувати 1 місяця з дати проведення заключної наради. За наявності обґрунтованих причин звіт може бути підготовлений у термін, що перевищує зазначений термін, з обов’язковим повідомленням про це заявника.

**7.4 Рішення щодо можливості (неможливості) видачі сертифіката**

Для прийняття рішення щодо сертифікації група з аудиту надає до ОС інформацію, яка охоплює:

* звіт про аудит;
* коментарі щодо невідповідностей і, де це застосовно, коригувань і коригувальних дій, вжитих заявником;
* підтвердження наданої органу з сертифікації 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.

ОС, в особі керівника ОС (особи, якій делеговане право на виконання його функцій), на підставі оцінки цієї інформації, приймає ***Рішення щодо можливості (неможливості) видачі сертифіката*** (Додаток 16).

ОС повинен впевнитись в тому, що інформація, надана групою з аудиту, є достатньою, а вжиті організацією коригування та коригувальні дії стосовно виявлених невідповідностей, є результативними. 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 планує та проводить ще один другий етап аудиту перед наданням рекомендацій щодо сертифікації.

Проект рішення візується виконавцем та підписується керівником ОС (особою, якій делеговане право на виконання цих функцій). У будь-якому випадку рішення приймає особа, яка не брала участі в проведенні аудиту та має відповідну компетентність.

***Примітка.*** *У разі прийняття рішення всупереч рекомендації групи з аудиту, підстави для прийняття такого рішення повинні бути обґрунтовані та задокументовані.*

У разі варіанта 1 (п. 7.3.3.1 цієї СП) ОС оформлює та реєструє в установленому порядку ***Сертифікат*** (Додаток 17), який видається заявнику. Інформація про виданий сертифікат розміщується на офіційному сайті ТОВ «ІМПЕРІУМ СЕРТИФІК».

У разі варіанта 2 (п. 7.3.3.1 цієї СП), якщо організація в термін, установлений ОС, усуне невідповідності та звернеться з повторною заявкою на сертифікацію, роботи з сертифікації можуть проводитись в повному або скороченому обсязі, коли перевіряють лише ті елементи СУІБ, стосовно яких були виявлені невідповідності. У разі ухвалення ОС позитивного рішення за результатами цих робіт, заявнику видається ***Сертифікат*** на СУІБ.

У разі варіанта 3 (п. 7.3.3.1 цієї СП) повторні роботи з сертифікації СУ організації проводяться за новою заявкою в повному обсязі.

Разом із сертифікатом ОС оформлює ліцензійну угоду на право застосування сертифікату та типову програму наглядового аудиту. Ліцензійна угода оформлюється в двох примірниках, візується виконавцем та підписується керівником ОС (особою, якій делеговане право на виконання цих функцій) та уповноваженим представником заявника. ***Типова програма наглядового аудиту*** (Додаток 16) розробляється за результатами робіт із сертифікації групою з аудиту під керівництвом керівника групи, підписується ними та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). З типовою програмою наглядового аудиту необхідно під підпис ознайомити уповноваженого представника заявника. Ліцензійна угода та типова програма наглядового аудиту оформлюються в двох примірниках: один комплект зберігається в ОС, другий передається заявнику.

Термін дії сертифіката на систему управління не продовжується.

Порядок та обсяг робіт з повторної сертифікації СУ визначений у р.9 цієї СП.

**8 ДІЯЛЬНІСТЬ ЩОДО НАГЛЯДАННЯ**

**8.1 Загальні положення**

Діяльність щодо наглядання за сертифікованими СУІБ організацій протягом усього терміну дії сертифіката здійснює ОС. Діяльність щодо наглядання передбачає проведення наглядових аудитів - аудитів на місці з метою оцінки дотримання сертифікованою СУІБ організації вимог ДСТУ ISO/IEC 27001. Ціллю нагляду є підтвердження, що схвалена СУІБ продовжує впроваджуватися, розгляд залучених змін до цієї системи, які були ініційовані як результат змін в роботі організації заявника та постійне підтвердження відповідності вимогам сертифікації.

Інші заходи з діяльності щодо наглядання можуть включати:

- запити до організації щодо аспектів сертифікації;

- аналізування заяв організації щодо її діяльності (наприклад, рекламних матеріалів, web-сайту та ін.),

- запити до організації щодо надання документів і записів (на паперових або електронних носіях) та їх аналізування,

- інші заходи моніторингу діяльності організації.

Наглядові аудити повинні проводитись щонайменше один раз на рік. Перший наглядовий аудит повинен бути проведений не пізніше 12 місяців від дати прийняття рішення щодо сертифікації.

Наглядовий аудит не обов’язково повинен передбачати проведення повного аудиту СУІБ.

**8.2 Проведення наглядових аудитів**

Обсяг, порядок та періодичність наглядових аудитів встановлюються ОС за результатами робіт із сертифікації та регламентуються типовою програмою наглядового аудиту, яка складається таким чином, щоб ОС мав можливість на регулярній основі здійснювати моніторинг діяльності, охопленої СУІБ, а також враховувати зміни в сертифікованій організації та її СУІБ.

Для проведення кожного конкретного наглядового аудиту ОС, на підставі типової програми наглядового аудиту, з урахуванням фактичного стану організації та результатів попередніх аудитів, розробляє ***Програму наглядового аудиту*** (Додаток 17), в якій визначає сферу наглядового аудиту та інші заходи з наглядових аудитів у разі їх застосування.

Програма нагляду повинна передбачати щонайменше розгляд наступних питань:

- елементи підтримки системи, такі як оцінку ризиків інформаційної безпеки та підтримку заходів безпеки, внутрішні аудити СУІБ і аналізування з боку керівництва;

* перевіряння дій, ужитих стосовно невідповідностей, що були виявлені під час попереднього аудиту;
* розглядання скарг;
* результативність СУІБ відповідно до досягнення сертифікованою організацією задач та намічених результатів СУІБ;
* постійний оперативний контроль,
* використовування знаків та/або будь-яких інших посилань на сертифікацію.

- зв’язки із зовнішніми сторонами, як це визначено СУІБ в ISO/IEC 27001, та іншими документами, визначеними для сертифікації;

- зміни в задокументованій системі;

- сфери, які підлягають змінам;

- вибрані вимоги ISO/IEC 27001;

- інші питання, за наявності.

Порядок визначення тривалості робіт із наглядання регламентований
***РІ-03 Визначення тривалості аудиту***

Роботи з діяльності щодо наглядання оплачуються заявником на підставі договору або додаткової угоди до договору, які укладаються в порядку, встановленому в п. 7.2.6 цієї СП.

Планування проведення наглядових аудитів за сертифікованими ОС СУІБ здійснюється шляхом складання відповідальною особою ОС ***Річних та Щомісячних планів–завдань на проведення наглядових аудитів за сертифікованими системами управління*** (далі – план наглядових аудитів). Виконавців робіт щодо підготовки та проведення наглядових аудитів визначає керівник ОС (особа, якій делеговане право на виконання цих функцій). Плани наглядових аудитів підписуються зазначеною відповідальною особою та затверджуються керівником ОС (особою, якій делеговане право на виконання цих функцій).

Для проведення наглядових аудитів формується група з аудиту в порядку, описаному в
п. 7.2.5 цієї СП. Відповідальним виконавцем є особа, прізвище якої зазначене в відповідній графі плану наглядового аудиту першим.

До початку проведення наглядового аудиту керівник групи з аудиту налагоджує попередній зв’язок з організацією та пропонує їй у разі наявності змін надати повідомлення про зміни та відповідні актуалізовані документи СУ. Група з аудиту під керівництвом керівника групи з аудиту здійснює аналізування наданих документів та іншої інформації (наприклад, рекламних матеріалів, web-сайту), а також результатів попередніх аудитів. Місце проведення аналізування документації визначає керівник групи з аудиту.

Одночасно з аналізуванням інформації, отриманої від організації, група з аудиту може організувати збір від незалежних джерел та аналізування додаткових відомостей, пов’язаних, наприклад, із виконанням організацією встановлених вимог щодо якості та безпечності послуги.

Під час кожного нагляду з боку ОС переглядається щонайменше таке:

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

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.

Результати аналізування документів та інформації враховуються при підготовці звіту за результатами наглядового аудиту.

Наглядовий аудит проводиться в порядку, описаному в п. 7.2.6.2 цієї СП. При цьому замість програми другого етапу аудиту, в тому ж порядку, з урахуванням зазначеного в п. 8.1 цієї СП, розробляється програма наглядового аудиту.

Якщо при проведенні наглядового аудиту виявлено невідповідності, керівник групи з аудиту повідомляє організацію про необхідність здійснення коригувань та/або коригувальних дій, надання документованих доказів їх виконання до ОС, а також проведення перевірки їх виконання (з відвідуванням або без відвідування організації).

Організація визначає, які коригування та/або коригувальні дії вона повинна виконати для усунення виявлених у результаті аудиту невідповідностей, узгоджує ці дії та термін їх виконання з керівником групи з аудиту та повідомляє ОС про їх здійснення.

***Звіт за результатами наглядового аудиту*** (Додаток 18) оформлюється в порядку, описаному в п. 7.3.3.1 цієї СП та повинен містити зокрема інформацію стосовно усунення невідповідностей, які було виявлено раніше, і версію Положення щодо застосовності, а також важливі зміни після попереднього аудиту. Замість рекомендації щодо можливості (неможливості) видачі сертифіката група з аудиту дає рекомендацію щодо можливості підтвердження, призупинення чи скасування дії сертифіката, а також, у разі потреби, щодо скорочення сфери сертифікації, разом з будь-якими умовами чи зауваженнями.

**8.3 Рішення за результатами діяльності щодо наглядання**

За результатами діяльності щодо наглядання ОС може підтвердити, призупинити, скасувати дію сертифіката, або скоротити сферу сертифікації (р. 11 цієї СП).

ОС, в особі керівника ОС (особи, якій делеговане право на виконання його функцій), на підставі оцінки інформації, наведеної в звіті за результатами наглядового аудиту, та будь – якої іншої інформації (наприклад, загальнодоступна інформація, коментарі від заявника про звіт), приймає та документує ***Рішення за результатами наглядового аудиту***, яке оформлюється за формою, наведеною в Додатку 21 до цієї СП. Проект рішення візується виконавцем та підписується керівником ОС (особою, якій делеговане право на виконання цих функцій). У будь – якому випадку рішення приймає особа, яка не брала участі в проведенні аудиту. Рішення оформлюється в двох примірниках: один зберігається в ОС, другий направляється заявнику.

***Примітка.*** *У разі прийняття рішення за результатами наглядового аудиту всупереч рекомендації групи з аудиту, підстави для прийняття такого рішення повинні бути обґрунтовані та задокументовані.*

**9 ПОВТОРНА СЕРТИФІКАЦІЯ**

Для отримання сертифіката на новий термін заявник подає в ОС заявку, як зазначено в
п. 7.2.1 цієї СП. Загальний порядок проведення робіт із сертифікації за поданою заявкою встановлений у розділі 7 цієї СП.

Заходи з повторної сертифікації повинні охоплювати аналіз звітів попередніх наглядових аудитів та результативності СУІБ протягом останнього циклу сертифікації.

Процедури аудиту повторної сертифікації повинні співпадати з тими, що їх застосовували під час первинного сертифікаційного аудиту СУІБ організації заявника, як описано в даній СП.

Час, дозволений для впровадження коригувальних дій, повинен бути погоджений із тяжкістю невідповідності та пов’язаним ризиком інформаційної безпеки.

**Примітка.** *ОС може проводити роботи з повторної сертифікації не в повному обсязі, передбаченому розділом 7 цієї СП, з урахуванням результатів нагядових аудитів, проведених протягом терміну дії сертифікату. Аудит на місці проводиться в будь – якому випадку.*

При проведенні робіт із повторної сертифікації ОС повинен враховувати:

* результативність СУ в цілому з урахуванням внутрішніх і зовнішніх змін та її постійної відповідності і придатності у сфері сертифікації;
* продемонстроване виконання зобов'язань підтримувати результативність і поліпшувати СУ для того, щоб удосконалювати усі показники;
* результативність СУ стосовно досягнення сертифікованою організацією цілей та запланованих результатів СУ.

Для суттєвих невідповідностей, виявлених під час проведення повторної сертифікації ОС визначає терміни для коригування та коригувальних дій. Такі дії повинні бути впроваджені та перевірені до закінчення дії сертифікації.

Якщо заходи з повторної сертифікації успішно завершено до закінчення терміну дії виданого сертифіката, термін дії нового сертифіката встановлюється на основі терміну дії наявного сертифіката. Новий сертифікат датується або днем прийняття рішення про повторну сертифікацію, або більш пізньою датою.

Якщо ОС не завершив аудит повторної сертифікації або не має можливості перевірити впровадження коригувань та коригувальних дій щодо суттєвих невідповідностей до дати завершення сертифікації, повторна сертифікація не рекомендується та дія сертифікату не подовжується. Організація інформується 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.

ОС приймає рішення щодо повторної сертифікації, ґрунтуючись як на результатах повторного сертифікаційного аудиту, так і на результатах перевіряння системи протягом дії сертифікації та скарг, отриманих від користувачів сертифікації.

**10 СПЕЦІАЛЬНІ АУДИТИ**

Діяльність, необхідна для здійснення спеціальних аудитів, підлягає спеціальним правилам, якщо організація із сертифікованою СУІБ зробила великі модифікації своєї системи або якщо були зроблені інші зміни, які можуть вплинути на основу її сертифікації.

**10.1 Розширення сфери сертифікації СУ**

Для розширення сфери сертифікації заявник подає в СП заявку, як зазначено в п. 7.2.1 цієї СП. Загальний порядок проведення робіт із сертифікації за поданою заявкою встановлений в розділі 7 цієї СП.

**Примітка 1.** ОС може проводити роботи з розширення сфери сертифікації не в повному обсязі, передбаченому розділом 7 цієї СП.

**Примітка 2.** ОС може проводити роботи з розширення сфери сертифікації в поєднанні з діяльністю щодо наглядання.

Порядок визначення тривалості робіт із розширення сфери сертифікації СУ регламентований ***РІ-03 Визначення тривалості аудиту.***

Роботи з розширення сфери сертифікації оплачуються заявником на підставі договору, який укладається в порядку, встановленому в п. 7.2.6 цієї СП.

**10.2 Короткострокові аудити**

ОС може ініціювати проведення короткострокових аудитів сертифікованої ним СУ в таких випадках:

- з метою перевірки усунення невідповідностей і виконання коригувальних дій за результатами попереднього аудиту;

- у разі отримання від організації повідомлення про зміни, що можуть негативно вплинути на відповідність СУ вимогам, що підтверджені під час сертифікації;

- з метою розслідування скарг, зокрема якщо результати аналізування скарги або будь-якої іншої інформації, включаючи приписи наглядових органів, свідчать про те, що СУ організації може не відповідати вимогам, що підтверджені під час сертифікації;

- з метою підтвердження можливості поновлення дії призупиненого сертифіката.

При прийнятті рішення щодо проведення короткострокового аудиту ОС письмово (не пізніше, ніж за 5 робочих днів до початку аудиту) сповіщає організацію про умови проведення аудиту та склад групи з аудиту. При прийнятті рішення щодо проведення короткострокового аудиту без попереднього повідомлення, ОС приділяє додаткову увагу складу групи з аудиту у зв’язку з відсутністю в організації можливості для його заперечення.

Короткострокові аудити проводяться в порядку, описаному в п.7.3.2 цієї СП, при цьому замість програми другого етапу аудиту в тому ж порядку розробляється програма аудиту. Результати оформлюються звітом про аудит в порядку, встановленому в п.7.3.3.1 цієї СП з урахуванням цілей аудиту.

**10.3 Дистанційні аудити**

У деяких випадках ОС може застосовувати дистанційний аудит – збір інформації, достатньої документації та її оцінка на відстані.

План аудиту повинен охоплювати діяльність з дистанційного аудиту, якщо це застосовується.

У випадках, коли будь-яка частина аудиту проводиться за допомогою електронного устаткування або ділянка, аудит якої необхідно провести є віртуальною, ОС забезпечує проведення таких заходів персоналом із відповідною компетентністю. Докази, отримані під час такого аудиту повинні бути достатніми щоб дозволити аудитору прийняти обґрунтоване рішення щодо відповідності вимогам, що перевіряються.

**11. СКОРОЧЕННЯ СФЕРИ СЕРТИФІКАЦІЇ, ПРИЗУПИНЕННЯ АБО СКАСУВАННЯ ДІЇ СЕРТИФІКАТА**

ОС скорочує сферу сертифікації СУІБ за наявності об’єктивних даних, які свідчать про те, що окремі частини цієї сфери постійно або суттєво не відповідають вимогам. Будь-яке скорочення сфери сертифікації СУІБ повинно бути узгоджене з вимогами ДСТУ ISO/IEC 27001:2015. При скороченні сфери сертифікації ОС скасовує діючий сертифікат, оформлює та реєструє, як зазначено в п. 7.3.3.3 цієї СП*,* новий сертифікат, з урахуванням внесених змін до сфери сертифікації. Термін дії сертифіката залишається незмінним.

ОС приймає та оформлює ***Рішення про призупинення дії або скасування дії сертифіката*** (Додаток 20) у випадках:

- виявлення невідповідності СУІБ вимогам ДСТУ ISO/IEC 27001:2015, зокрема, вимогам щодо результативності;

- наявності обґрунтованих претензій споживачів послуги;

- виявлення неправильного використання сертифіката;

- виявлення порушень правил або процедур, установлених ОС, зокрема відмова організації проводити наглядові аудти або повторні сертифікаційні аудити з необхідною періодичністю;

- сертифікована організація добровільно подала прохання щодо призупинення.

Рішення про призупинення дії сертифіката оформлюється в двох примірниках відповідальним виконавцем ОС та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). В рішенні зазначаються умови, за яких дію сертифіката може бути поновлено. Один примірник рішення зберігається в ОС, другий – надається організації. Під час призупинення дії сертифіката організація не має права посилатися на свій сертифікований статус.

ОС поновлює призупинену сертифікацію, якщо проблемне питання, результатом якого є призупинення, вирішено. Якщо організація не вирішила проблемне питання, результатом якого було призупинення, в термін до шести місяців, дія сертифіката скасовується або скорочується сфера сертифікації.

Перевірку виконання умов, за яких дію сертифіката може бути поновлено, ОС може здійснювати шляхом аналізування наданих організацією підтверджувальних документів і/або проведенням короткострокового аудиту, як зазначено в п.10.2 цієї СП. За позитивних результатів перевірки ОС приймає ***Рішення про поновлення дії сертифіката*** (Додаток 20), яке оформлюється в двох примірниках відповідальним виконавцем ОС та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). Один примірник рішення зберігається в ОС, другий – надається організації. За негативних результатів перевірки, в залежності від ступеня відповідності СУ встановленим вимогам, ОС скорочує сферу сертифікації або приймає рішення про скасування дії сертифіката, яке оформлюється в двох примірниках відповідальним виконавцем ОС та затверджується керівником ОС (особою, якій делеговане право на виконання цих функцій). Один примірник рішення зберігається в ОС, другий – направляється організації.

ОС приймає рішення про скасування дії сертифіката у випадках:

- якщо результати діяльності з наглядання свідчать про принципову невідповідність СУІБ встановленим вимогам;

- якщо у разі зміни вимог до сертифікації організація не може забезпечити відповідність новим вимогам;

- якщо організація протягом тривалого часу (більше ніж 6 місяців) не здійснює діяльність, охоплену сферою сертифікації;

- якщо заявник не виконує свої фінансові зобов'язання перед ОС (наприклад стосовно оплати за проведення робіт із сертифікації, наглядових аудитів);

- якщо організація в терміни, які були узгоджені з ОС, не усунула причини, з яких дію сертифіката було призупинено;

- за бажанням організації.

У разі скасування дії сертифіката організація не має права посилатися на свій сертифікований статус та повинна повернути ОС оригінал сертифіката, який підлягає знищенню.