Національне агентство з акредитації України

Затверджено
Наказом НААУ
від 09.09.2016 № 215-Я

ЗАГАЛЬНИЙ ДОКУМЕНТ

Інформаційні технології - Методи забезпечення безпеки - Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки (згідно ISO/IEC 27006:2015)

Передмова

ISO (Міжнародна організація зі стандартизації) і IEC (Міжнародна електротехнічна комісія) утворюють спеціалізовану систему міжнародної стандартизації. Національні органи, які є членами ISO або IEC приймають участь у розробці міжнародних стандартів через технічні комітети, створені відповідною організацією для вирішення конкретних питань в областях технічної діяльності. Технічні комітети ISO та IEC співпрацюють в областях, що становлять взаємний інтерес. Інші міжнародні організації, урядові та неурядові, які мають зв'язки з ISO та IEC, також беруть участь в роботі. В області інформаційних технологій, ISO та IEC створили спільний технічний комітет ISO/IEC JTC1.

Процедури, використані для розробки даного, а також процедури, призначені для його подальшої підтримки описано в частині 1 Директив ISO/IEC. Зокрема, до уваги слід прийняти критерії затвердження, що різняться залежно від типу документу. Даний документ було створено у відповідності до редакційних правил частини 2 Директив ISO/IEC.

Слід звернути увагу на те, що деякі з елементів цього документа можуть бути об'єктом патентних прав. ISO та IEC не несуть відповідальності за ідентифікацію будь-яких або всіх таких патентних прав. Деталі щодо будь-яких патентних прав, визначених під час розробки документу наводяться у Вступі та/або у переліку отриманих патентних декларацій (див. www.iso.org/patents).

Будь-яка торгова марка, використана у даному документі є інформацією, наведеною для зручності користувачів і не означає схвалення такої торгової марки.

Для отримання пояснення щодо значення окремих термінів та виразів ISO, що відносяться до оцінки відповідності, а також інформації щодо дотримання ISO принципів ВТО щодо технічних бар'єрів в торгівлі, див. наступне посилання: Foreword – Supplementary information.

Комітетом, що відповідає за цей документ є ISO/IEC JTC 1 «Інформаційні технології», підкомітет SC 27, «Методи IT безпеки».

ISO/IEC 27006 був підготовлений спільним технічним комітетом ISO/IEC JTC 1, «Інформаційні технології», Підкомітет SC 27, «Методи IT безпеки».

Це третє видання скасовує та замінює друге видання (ISO/IEC 27006:2011), яке було технічно переглянуте.

Вступ

ISO/IEC 17021-1 встановлює критерії для органів, що здійснюють аудит і сертифікацію систем менеджменту. Якщо такі органи проходять акредитацію відповідно до ISO/IEC 17021-1 з метою аудиту та сертифікації систем менеджменту інформаційною безпекою (СМІБ) відповідно до ISO/IEC 27001:2013, деякі додаткові вимоги та настанови до стандарту ISO/IEC 17021-1 є необхідними. Їх надає цей міжнародний стандарт.

Текст в цьому міжнародному стандарті відповідає структурі ISO/IEC 17021-1, а додаткові специфічні вимоги щодо СМІБ та настанови щодо застосування ISO/IEC 17021-1 для сертифікації СМІБ позначаються буквами "IS".

Термін "shall"(повинні) використовується в цьому стандарті для позначення тих положень, які, відображуючи вимоги ISO/IEC 17021-1 та ISO/IEC 27001, є обов'язковими. Термін "should" (слід) використовується для вказівки на рекомендацію.

Основною метою цього міжнародного стандарту є сприяння органам з акредитації для більш ефективної гармонізації застосування стандартів, на відповідність яким вони проводять оцінку органів з сертифікації.

В даному міжнародному стандарті терміни "система менеджменту" і "система" є взаємозамінними. Визначення системи менеджменту знаходиться в ISO 9000:2005. Систему менеджменту в значенні, в якому вона використовується в цьому міжнародному стандарті, не слід плутати з іншими видами систем, таких як IT системи.

Інформаційні технології - Методи забезпечення безпеки - Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки

1 Сфера дії

Цей міжнародний стандарт встановлює вимоги і надає керівництво для органів, які провадять аудит і сертифікацію систем менеджменту інформаційної безпеки (СМІБ), на додаток до вимог, що містяться в ISO/IEC 17021-1 та ISO/IEC 27001. В першу чергу він призначений для підтримки акредитації органів з сертифікації, що забезпечують сертифікацію СМІБ.

Вимоги, що містяться в даному міжнародному стандарті повинні бути продемонстровані з врахуванням компетентності та надійності будь-яким органом, що здійснює сертифікацію СМІБ. Настанови, що містяться в даному міжнародному стандарті надають додаткове тлумачення зазначених вимог для будь-якого органу, що здійснює сертифікацію СМІБ.

ПРИМІТКА Цей міжнародний стандарт може бути використаний в якості нормативного документу при акредитації, паритетному оцінюванні або інших процесах аудиту.

2 Нормативні посилання

Даний документ містить нормативні посилання на нижченаведені документи (повністю або частково), які є обов'язковими при застосуванні цього документу. Для датованих посилань застосовується тільки видання, на яке посилаються. Для недатованих посилань застосовують останнє видання документу, на який здійснено посилання (включаючи будь-які поправки).

ISO/IEC 17021-1:2015 «Оцінка відповідності - Вимоги до органів, які здійснюють аудит і сертифікацію систем менеджменту»

ISO/IEC 27000 «Інформаційні технології - Методи забезпечення безпеки - Системи менеджменту інформаційної безпеки – Огляд та словник»

ISO/IEC 27001:2013 «Інформаційні технології - Методи забезпечення безпеки - Системи менеджменту інформаційної безпеки – Вимоги»

3 Терміни та визначення

3.1
Документи щодо сертифікації
документи, які вказують на те, що СМІБ організації-клієнта відповідає зазначеним стандартам СМІБ і будь-яким додатковим документам, що вимагаються в рамках даної системи

4 Принципи

Застосовуються принципи, викладені в ISO/IEC 17021-1, п. 4.

5 Загальні вимоги

5.1 Правові та договірні питання

Застосовуються вимоги з ISO/ IEC 17021-1, п. 5.1.

5.2 Менеджмент неупередженості

Застосовуються вимоги ISO/IEC 17021-1, п. 5.2. Крім того, застосовуються наступні вимоги і настанови щодо СМІБ.

5.2.1 IS 5.2 Конфлікти інтересів

Органи з сертифікації можуть виконувати наступні обов'язки, які не розглядаються як консалтингова діяльність або потенційний конфлікт інтересів:

a) організація та участь в якості лектора в навчальних курсах, за умови, що такі курси відносяться до менеджменту інформаційної безпеки, пов'язаних з системами менеджменту або проведенням аудиту, на яких органи з сертифікації повинні обмежуватися наданням загальної інформації та рекомендацій, що знаходяться у вільному доступі, тобто вони не надають консультацій конкретній компанії, що суперечить вимогам підпункту b) нижче;

b) надання або публікація на запит інформації, яка описує інтерпретацію органу з сертифікації вимог стандартів щодо аудиту сертифікації (див. 9.1.3.6);

c) діяльність, що передує аудиту, спрямована виключно на визначення готовності до аудиту сертифікації; однак така діяльність не повинна призводити до надання рекомендацій або порад, які суперечили б цьому пункту і орган з сертифікації повинен бути в змозі підтвердити, що така діяльність не суперечить цим вимогам, і, що вони не використовуються для виправдання скорочення кінцевої тривалості сертифікаційного аудиту;

d) проведення аудиту другої і третьої сторони відповідно до стандартів або нормативних документів, що відрізняються від тих, що є частиною сфери акредитації;

e) робити свій внесок під час сертифікаційних аудитів та наглядів, наприклад, шляхом виявлення можливостей для поліпшення, так як вони стають очевидними під час аудитів, без надання рекомендацій щодо конкретних рішень.

Орган з сертифікації не повинен здійснювати аналіз безпеки внутрішньої інформації СМІБ клієнта, яка є об’єктом сертифікації. Більше того, орган з сертифікації повинен бути незалежним від органу або органів (включаючи будь-яких осіб), які забезпечують внутрішній аудит СМІБ.

5.3 Відповідальність та фінансування

Застосовуються вимоги ISO/IEC 17021-1, пункт 5.3.

6 Структурні вимоги

Застосовуються вимоги ISO/IEC 17021-1, розділ 6.

7 Вимоги до ресурсів

7.1 Компетентність персоналу

Застосовуються вимоги ISO/IEC 17021-1, п. 7.1. Додатково застосовуються наступні вимоги та настанови.

7.1.1 IS 7.1.1 Загальні положення

7.1.1.1 Загальні вимоги до компетентності

Орган з сертифікації повинен забезпечити наявність знань щодо технологічних, правових та регуляторних розробок, що стосуються СМІБ організації-клієнта, яку він оцінює.

Орган з сертифікації повинен визначити вимоги до компетентності щодо кожної функції сертифікації, які зазначено в Таблиці A.1 ISO/IEC 17021-1. Орган з сертифікації повинен приймати до уваги всі вимоги, що мають відношення до визначених органом з сертифікації

технічних областей СМІБ та викладені в ISO/IEC 17021-1, а також п.7.1.2 і п.7.2.1 цього міжнародного стандарту.

ПРИМІТКА Додаток А надає загальну інформацію щодо вимог до компетентності для персоналу, залученого до окремих функцій сертифікації.

7.1.2 IS 7.1.2 Визначення критеріїв компетентності

7.1.2.1 Вимоги до компетентності для проведення аудиту СМІБ

7.1.2.1.1 Загальні вимоги

Орган з сертифікації повинен мати критерії для перевірки попереднього досвіду, спеціального навчання або інструктажу членів групи з аудиту, які забезпечують принаймні наступне:

a) знання щодо безпеки інформації;
b) технічні знання щодо діяльності, аудит якої проводиться;
c) знання щодо систем менеджменту;
d) знання принципів проведення аудиту;
   ПРИМІТКА подальша інформація щодо принципів проведення аудиту знаходиться в ISO 19011.
e) Знання щодо моніторингу, вимірювання, аналізу та оцінювання СМІБ.

Вищевикладені вимоги підпунктів з a) по e) застосовуються до усіх аудиторів, залучених до групи з аудиту за винятком підпункту b), виконання якого можливо поділити між всіма аудиторами, які є членами аудиторської групи.

Група з аудиту повинна мати компетентність для відслідковування ознак інцидентів інформаційної безпеки в СМІБ клієнта до відповідних елементів СМІБ.

Група з аудиту повинна мати належний досвід роботи щодо вищезазначених пунктів, а також досвід щодо практичного застосування цих пунктів (це не означає, що аудитор повинен володіти повним діапазоном досвіду у всіх областях інформаційної безпеки, але група з аудиту в цілому повинна мати достатнє розуміння та досвід для охоплення сфери СМІБ, щодо якої проводиться аудит).

7.1.2.1.2 Термінологія, принципи, практика та методи менеджменту інформаційної безпеки

Група з аудиту повинна мати сумарні знання щодо:

a) структури, ієрархії та взаємозв'язків спеціальної документації СМІБ;
b) інструментів, засобів, методів, що відносяться до менеджменту інформаційної безпеки, та їх застосування;
c) оцінка та менеджмент ризиків інформаційної безпеки;
d) процеси, застосовні до СМІБ;
e) сучасні технології, в яких інформаційна безпека є актуальною або може стати проблемним питанням.

Кожен аудитор повинен відповідати підпунктам a), c) та d).

7.1.2.1.3 Стандарти та нормативні документи щодо систем менеджменту інформаційної безпеки

Аудитори, залучені до аудиту СМІБ повинні мати знання щодо:

a) всіх вимог, що містяться в ISO/IEC 27001.
Група з аудиту повинна мати сумарні знання щодо:

b) усіх засобів контролю, що містяться в ISO/IEC 27002 (а також із спеціальних секторальних стандартів, якщо це визначено як необхідність) та їх впровадження. Зазначені засоби поділяються на наступне:

1) політики щодо інформаційної безпеки;
2) організація інформаційної безпеки;
3) безпека людських ресурсів;
4) менеджмент активів;
5) контроль доступу, включаючи авторизацію;
6) криптографія;
7) фізична безпека та безпека навколишнього середовища;
8) безпека діяльності, включаючи іт послуги;
9) безпека зв'язку, включаючи менеджмент безпеки мережі та передачі інформації;
10) придбання, розробка та підтримка системи;
11) відносини із постачальником, охоплюючи послуги, що виконуються на умовах аутсорсингу;
12) менеджмент інцидентів, пов'язаних із інформаційною безпекою;
13) менеджмент аспектів інформаційної безпеки щодо постійності діяльності, охоплюючи надлишок потужностей;
14) відповідність, включаючи аналіз інформаційної безпеки.

7.1.2.1.4 Практика менеджменту бізнеса

Аудитори, залучені до аудиту СМІБ, повинні мати знання щодо:

a) сталої практики галузі інформаційної безпеки та процедур інформаційної безпеки;
b) політик та вимог бізнесу щодо інформаційної безпеки;
c) загальних концепцій менеджменту бізнесу, практик та взаємозв'язку між політикою, цілями та результатами;
d) процесу менеджменту та пов'язаної термінології.

ПРИМІТКА Ці процеси також включають менеджмент людських ресурсів, внутрішнє та зовнішнє інформування та інші відповідні допоміжні процеси.

+

7.1.2.1.5 Бізнес сектор клієнта

Аудитори, залучені до аудиту СМІБ, повинні мати знання щодо:

a) законодавчих та регуляторних вимог у конкретній галузі інформаційної безпеки, географічного регіону та юрисдикції(цій);
ПРИМІТКА Знання законодавчих та регуляторних вимог не вимагає наявності досвіду у законодавчій сфері.
b) ризиків щодо інформаційної безпеки відповідно до сектору бізнесу;
c) основної термінології, процесів та технологій відповідно до бізнес сектору клієнта;
d) відповідної практики в бізнес секторі.
Критерій а) може бути розподіллено між групою з аудиту

7.1.2.1.6 Продукція процеси та організація клієнта

Загалом, аудитори, залучені до проведення аудиту СМІБ, повинні мати знання щодо:

a) впливу типу, розміру, способу управління, структури, функцій та відносин організації на розробку та впровадження СМІБ та сертифікаційної діяльності, включаючи аутсорсинг;

b) комплексної діяльності у широкій перспективі;
c) законодавчих та регуляторних вимог, застосовних до продукції або послуги.

7.1.2.2 Вимоги до компетентності щодо керування групою з аудиту СМІБ

На додаток до вимог п. 7.1.2.1, керівники групи з аудиту повинні відповідати наступним вимогам, що необхідно продемонструвати під час аудитів під наглядом та керівництвом (іншого аудитора):

a) Знання та навички щодо керування процесом аудиту та групою з аудиту;
b) Демонстрація спроможності ефективного спілкування як усно так і письмово.

7.1.2.3 Вимоги до компетентності для здійснення аналізу заявки

7.1.2.3.1 Стандарти та нормативні документи щодо системи менеджменту інформаційної безпеки

Персонал, що здійснює аналіз заявки для визначення необхідної компетентності групи з аудиту з метою відбору членів групи з аудиту та визначення часу аудиту, повинен мати знання щодо:

а) відповідних стандартів СМІБ та інших нормативних документів, що використовуються в процесі сертифікації.

7.1.2.3.2 Сектор діяльності клієнта

Персонал, що здійснює аналіз заявки для визначення необхідної компетентності групи з аудиту з метою відбору членів групи з аудиту та визначення часу аудиту, повинен мати знання щодо:

а) основної термінології, процесів, технологій та ризиків відповідно сектору діяльності клієнта.

7.1.2.3.3 Продукція, процеси та організація клієнта

Персонал, що здійснює аналіз заявки для визначення необхідної компетентності групи з аудиту з метою відбору членів групи з аудиту та визначення часу аудиту, повинен мати знання щодо:

а) продукції, процесів, організаційного типу, розміру, способу управління, структури, функцій та відносин клієнта щодо розробки та впровадження СМІБ та сертифікаційної діяльності включаючи аутсорсинг;

7.1.2.4 Вимоги до компетентності щодо аналізу звітів про аудит та прийняття рішень щодо сертифікації

7.1.2.4.1 Загальні положення

Персонал, що здійснює аналіз звітів про аудит та приймає рішення щодо сертифікації, повинен мати знання, які дозволяють такому персоналу перевіряти придатність сфери сертифікації, а також перевіряти зміни до сфери та їх вплив на ефективність аудиту, зокрема, на постійну правильність визначення інтерфейсів та підпорядкованості і споріднених з цим ризиків.

Додатково, персонал що здійснює аналіз звітів про аудит та приймає рішення щодо сертифікації, повинен мати знання щодо:

a) систем менеджменту загалом;
b) процесів та процедур аудиту;

c) принципів, практик та методів аудиту.

7.1.2.4.2 Термінологія, принципи, практики та методи менеджменту інформаційної безпеки

Персонал, що здійснює аналіз звітів про аудит та приймає рішення щодо сертифікації повинен мати знання щодо:

a) позицій, перелічених у п. 7.1.2.1.2 a), c) та d);

b) законодавчих та регуляторних вимог, що стосуються інформаційної безпеки.

7.1.2.4.3 Стандарти та нормативні документи щодо систем менеджменту інформаційної безпеки

Персонал, що здійснює аналіз звітів про аудит та приймає рішення щодо сертифікації повинен мати знання щодо:

a) відповідних стандартів СМІБ та інших нормативних документів, що використовуються в процесі сертифікації.

7.1.2.4.4 Сектор діяльності клієнта

Персонал, що здійснює аналіз звітів про аудит та приймає рішення щодо сертифікації повинен мати знання щодо:

a) основної термінології, процесів, технологій та ризиків відповідно сектору діяльності клієнта.

7.1.2.4.5 Продукція процеси та організація клієнта

Персонал, що здійснює аналіз звітів про аудит та приймає рішення щодо сертифікації повинен мати знання щодо:

a) продукції, процесів, організаційного типу, розміру, способу управління, структури, функцій та відносин клієнта.

7.2 Персонал, залучений до робіт з сертифікації

Застосовуються вимоги ISO/IEC 17021-1, пункт 7.2 Крім того, застосовуються наступні вимоги і настанови.

7.2.1 IS 7.2 Демонстрація знань та досвіду аудитора

Орган з сертифікації повинен продемонструвати, що його аудитори мають знання та досвід за допомогою:

a) визнаної кваліфікації, характерної для СМІБ;
b) реєстрації в якості аудитора, де це застосовно;
c) участі у навчаннях щодо СМІБ та отримання відповідних персональних підтверджуючих документів;
d) актуальних записів щодо професійного розвитку;
e) аудитів СМІБ, за якими провів спостереження інший аудитор СМІБ.

7.2.1.1 Відбір аудиторів

На додаток до п. 7.1.2.1, критерії щодо відбору аудиторів повинні забезпечувати, що кожен аудитор:

a) має професійну освіту або навчання рівня, який є еквівалентним університетській освіті;
b) має щонайменше чотири роки досвіду на штатній посаді в сфері інформаційних технологій, з яких щонайменше два роки в ролі або з функціями, щодо інформаційної безпеки;
c) завершив щонайменше п'ятиденне навчання, яке охоплює аудити СМІБ та менеджмент аудитів;
d) набув досвіду у всьому процесі оцінки інформаційної безпеки до того як взяв на себе відповідальність виконувати обов'язки в якості аудитора. Слід, щоб такий досвід був отриманий шляхом прийняття участі щонайменше у чотирьох аудитах сертифікації СМІБ, включаючи повторну сертифікацію та наглядові аудити, які налічують загалом 20 днів, з яких наглядами можуть бути максимум 5 днів. Участь повинна включати аналіз документації та оцінку ризиків, оцінку впровадження та звітність щодо аудиту;
e) має відповідний та актуальний досвід;
f) підтримує наявні знання та навички щодо інформаційної безпеки та проведення аудитів шляхом безперервного професійного розвитку.

Технічні експерти повинні відповідати критеріям a), b) та e).

7.2.1.2 Відбір аудиторів для керування групою з аудиту

На додаток до п. 7.1.2.2 та 7.2.1.1, критерії щодо відбору аудитора для керування групою повинні забезпечувати, що такий аудитор:

a) прийняв активну участь у всіх етапах щонайменше трьох аудитів СМІБ. Прийняття участі повинне включати первинне визначення сфери та планування, аналіз документації та оцінку ризиків, оцінку впровадження та офіційну звітність щодо аудиту.

7.3 Залучення окремих зовнішніх аудиторів та зовнішніх технічних експертів

Застосовуються вимоги ISO/IEC 17021-1, пункт 7.3. Додатково застосовуються наступні вимоги та настанови.

7.3.1 IS 7.3 Залучення зовнішніх аудиторів або зовнішніх технічних експертів в якості членів групи з аудиту

Технічні експерти повинні працювати під керівництвом аудитора. Мінімальні вимоги до технічних експертів перелічено в п. 7.2.1.1.

7.4 Записи щодо персоналу

Застосовуються вимоги ISO/IEC 17021-1, пункт 7.4.

7.5 Аутсорсинг

Застосовуються вимоги ISO/IEC 17021-1, пункт 7.5.

8 Вимоги до інформації

8.1 Інформація, що знаходиться у відкритому доступі

Застосовуються вимоги ISO/IEC 17021-1, пункт 8.1.

8.2 Документи щодо сертифікації

Застосовуються вимоги ISO/IEC 17021-1, пункт 8.2. Додатково застосовуються наступні вимоги та настанови.

8.2.1 IS 8.2 Документи щодо сертифікації СМІБ

Документи щодо сертифікації повинні бути підписані посадовою особою, на яку покладено таку відповідальність. Версія Положення про застосовність має бути включена до документів щодо сертифікації.

ПРИМІТКА Зміни до Положення про застосовність, які не змінюють сферу сертифікації, не вимагають актуалізації документу щодо сертифікації.

Визначення конкретних стандартів, що використовуються для визначеного сектору, також може бути включено до документів щодо сертифікації.

8.3 Посилання на сертифікацію та використання знаків

Застосовуються вимоги ISO/IEC 17021-1, пункт 8.3.

8.4 Конфіденційність

Застосовуються вимоги ISO/IEC 17021-1, пункт 8.4. Додатково застосовуються наступні вимоги та настанови.

8.4.1 IS 8.4 Доступ до організаційних записів

Перед проведенням аудиту сертифікації орган з сертифікації повинен направити запит до клієнта щодо повідомлення того, чи наявна будь-яка інформація щодо СМІБ (такі як записи щодо СМІБ або проектування та ефективності контролю), яка не може бути надана для аналізу аудиторською групою, так як містить конфіденційну інформацію або інформацію з обмеженим доступом. Орган з сертифікації повинен визначити, чи може бути проведено повноцінний аудит СМІБ за відсутності вказаних документів. Якщо орган з сертифікації зробить висновок щодо неможливості повноцінного проведення аудиту СМІБ без розгляду інформації, визначеної як конфіденційна або інформації з обмеженим доступом, він повинен попередити організацію клієнта, що сертифікаційний аудит не може бути проведено доки не будуть забезпечені заходи щодо надання відповідного доступу.

8.5 Обмін інформацією між органом з сертифікації та його клієнтами

Застосовуються вимоги ISO/IEC 17021-1, п. 8.5.

9 Вимоги до процесу

9.1 Перед-сертифікаційні заходи

9.1.1 Заявка

Застосовуються вимоги ISO/IEC 17021-1, п. 9.1.1. Додатково застосовуються наступні вимоги та настанови.

9.1.1.1 IS 9.1.1 Готовність заявки

Орган з сертифікації повинен вимагати від клієнта мати задокументовану та впроваджену СМІБ, яка відповідає ISO/IEC 27001 та іншим документам, необхідним для сертифікації.

9.1.2 Аналіз заявки

Застосовуються вимоги ISO/IEC 17021-1, п. 9.1.2.

9.1.3 Програма аудиту

Застосовуються вимоги ISO/IEC 17021-1, п. 9.1.3. Додатково застосовуються наступні вимоги та настанови.

9.1.3.1 IS 9.1.3 Загальні положення

Програма аудитів для СМІБ повинна враховувати визначені засоби контролю інформаційної безпеки.

9.1.3.2 IS 9.1.3 Методологія аудиту

Процедури органу з сертифікації не повинні передбачати конкретний спосіб впровадження СМІБ або конкретний формат для документації та записів. Процедури сертифікації повинні зосереджуватись на встановлені того, що СМІБ клієнта відповідає вимогам, визначеним в ISO/IEC 27001 та політикам і цілям клієнта.

ПРИМІТКА Подальші настанови щодо проведення аудиту викладені в ISO/IEC 27007.

9.1.3.3 IS 9.1.3 Загальна підготовка до первинного аудиту

Орган з сертифікації повинен вимагати, щоб клієнт прийняв всіх необхідних заходів для надання доступу до звітів про внутрішній аудит та звітів щодо незалежного аналізу інформаційної безпеки.

Протягом етапу 1 аудиту сертифікації клієнт повинен надати щонайменше наступну інформацію:

a) загальна інформація щодо СМІБ та діяльності, яку вона охоплює;

b) примірник необхідної документації СМІБ, вказаної в ISO/IEC 27001 та, де це необхідно, пов’язаної документації.

9.1.3.4 IS 9.1.3 Періодичність аналізу

Орган з сертифікації не повинен сертифікувати СМІБ, якщо та не пройшла хоча б один аналіз з боку керівництва та один внутрішній аудит СМІБ, які б охоплювали сферу сертифікації.

9.1.3.5 IS 9.1.3 Сфера сертифікації

Група з аудиту повинна проводити аудит СМІБ клієнта з охопленням визначеної сфери відповідно до всіх застосовних вимог до сертифікації. Орган з сертифікації повинен підтвердити у сфері СМІБ клієнта, що клієнт відповідає вимогам, встановленим п. 4.3 ISO/IEC 27001.

Органи з сертифікації повинні забезпечувати, щоб оцінка ризиків інформаційної безпеки клієнта та усунення таких ризиків відповідним чином відображала його (клієнта) діяльність та розповсюджувалась на всю його діяльність, визначену сферою сертифікації. Органи з сертифікації повинні підтверджувати, що зазначене відображено у сфері СМІБ клієнта та Положенні про застосовність. Орган з сертифікації повинен перевірити, що для кожної сфери сертифікації наявне хоча одне Положення про застосовність.

Органи з сертифікації повинні забезпечувати, щоб інтерфейси щодо послуг та діяльності, які не в повному обсязі знаходяться в межах сфери СМІБ, були зазначені в СМІБ, яка є предметом сертифікації, та включені до оцінки ризиків інформаційної безпеки клієнта. Прикладом зазначеної ситуації є сумісне використання ресурсів (наприклад, IT систем, баз

даних та телекомунікаційних систем або передавання виробничих функцій на умовах аутсорсингу) з іншими організаціями.

9.1.3.6 IS 9.1.3 Критерії аудиту сертифікації

Критерієм, відповідно до якого проводиться аудит СМІБ клієнта, повинен бути стандарт щодо СМІБ ISO/IEC 27001. Залежно від виконуваної функції, для сертифікації можуть бути необхідні інші документи.

9.1.4 Визначення часу аудиту

Застосовуються вимоги ISO/IEC 17021-1, п. 9.1.4. Додатково застосовуються наступні вимоги та настанови.

9.1.4.1 IS 9.1.4 Час аудиту

Органи з сертифікації повинні надавати аудиторам достатній час для вжиття всіх заходів щодо первинного аудиту, наглядового аудиту або аудиту повторної сертифікації. Розрахунок загального часу аудиту повинен включати достатній час для звітування за результатами аудиту.

Орган з сертифікації повинен використовувати Додаток B для визначення часу аудиту.

ПРИМІТКА Подальші настанови та приклади розрахунку часу аудиту надано у Додатку C.

9.1.5 Вибірка при розгалуженій структурі

Застосовуються вимоги ISO/IEC 17021-1, п. 9.1.5. Додатково застосовуються наступні вимоги та настанови.

9.1.5.1 IS 9.1.5 Розгалужена структура (декілька ділянок)

9.1.5.1.1 Якщо клієнт має ряд ділянок, які відповідають критеріям з a) по c), зазначеним нижче, органи з сертифікації можуть розглянути можливість застосування підходу, що ґрунтується на вибірці для аудиту сертифікації при розгалуженій структурі:

a) Всі ділянки діють відповідно до однієї СМІБ, яка керується та піддається аудиту централізовано та є об’єктом централізованого аналізу з боку керівництва;
b) Всі ділянки включено у внутрішню програму аудитів СМІБ клієнта;
c) Всі ділянки включено у програму аналізу СМІБ клієнта з боку керівництва.

9.1.5.1.2 Орган з сертифікації, який бажає використати підхід, що ґрунтується на вибірці, повинен мати процедури, які забезпечують наступне:

a) первинний аналіз договору визначає, в максимально можливій мірі, відмінності між дільницями таким чином щоб визначити достатній рівень вибірки.
b) органом з сертифікації було відібрано достатню кількість ділянок, приймаючи до уваги:
    1) результати внутрішніх аудитів головного офісу та ділянок;
    2) результати аналізу з боку керівництва;
    3) відмінності у розмірі ділянок;
    4) відмінності у виробничому призначені ділянок;
    5) складність інформаційних систем на різних ділянках;
    6) відмінності у методах роботи;

7) відмінності у діяльності, що здійснюється;
8) відмінності у проектуванні та здійснення контролю;
9) потенційна взаємодія із критичними інформаційними системами або інформаційними системами, що обчислюють інформацію із обмеженим доступом;
10) будь-які законодавчі вимоги, що різняться;
11) географічні та культурні аспекти;
12) ситуація, пов'язана із ризиками на дільницях;
13) інциденти щодо інформаційної безпеки на окремих ділянках.

c) Достатня вибірка здійснена серед усіх ділянок в межах сфери СМІБ клієнта; такий відбір повинен ґрунтуватись на суб'єктивному виборі для відображення факторів, представлених у вищезазначеному підпункті b), а також на елементі випадковості.
d) аудит кожної ділянки, яка є об'єктом значних ризиків, включеної до СМІБ, проводиться органом з сертифікації до надання сертифікації.
e) програму аудиту було спроектовано у світлі вищезазначених вимог і вона охоплює достатню вибірку відповідно до сфери сертифікації СМІБ в межах трирічного періоду.
f) у випадку встановлення невідповідності у головному офісі або на окремій ділянці, процедура щодо коригувальних дій застосовується до головного офісу та всіх ділянок, охоплених сертифікатом.

Аудит повинен стосуватися діяльності головного офісу клієнта для забезпечення того, що єдина СМІБ застосовується до всіх ділянок і забезпечує централізований менеджмент на операційному рівні. Аудит повинен стосуватися усіх проблем, окреслених вище.

9.1.6 Декілька систем менеджменту

Застосовуються вимоги ISO/IEC 17021-1, п. 9.1.6. Додатково застосовуються наступні вимоги та настанови.

9.1.6.1 IS 9.1.6 Інтеграція документації СМІБ із документацією інших систем менеджменту

Орган з сертифікації може прийняти комбіновану документацію (наприклад, щодо інформаційної безпеки, якості, здоров'я та безпеки і навколишнього середовища) до тих пір поки СМІБ є чітко визначеною разом із належними інтерфейсами по відношенню до інших систем.

9.1.6.2 IS 9.1.6 Комбінування аудитів систем менеджменту

Аудит СМІБ можливо комбінувати із аудитами інших систем менеджменту, за умови того, що аудит задовольняє всім вимогам щодо сертифікації СМІБ. Всі важливі для СМІБ елементи повинні бути чіткими та такими, які легко визначити у звітах про аудит. Комбінація аудитів не повинна негативно впливати на якість аудиту.

9.2 Планування аудитів

9.2.1 Визначення цілей, сфери та критеріїв аудиту

Застосовуються вимоги ISO/IEC 17021-1, п. 9.2.1. Додатково застосовуються наступні вимоги та настанови.

9.2.1.1 IS Цілі аудиту

Цілі аудиту повинні включати визначення ефективності системи менеджменту для забезпечення того, що клієнт, ґрунтуючись на аналізу ризиків, впровадив застосовний контроль та досягнув поставлених цілей в області інформаційної безпеки.

9.2.2 **Відбір та призначення групи аудиту**

Застосовуються вимоги ISO/IEC 17021-1, п. 9.2.2. Додатково застосовуються наступні вимоги та настанови.

9.2.2.1 IS 9.2.2 Компетентність групи з аудиту

Застосовуються вимоги, перелічені в п. 7.1.2. Для діяльності з нагляду та спеціальних аудитів застосовуються тільки ті вимоги, що відносяться до запланованої діяльності з нагляду та спеціальних аудитів.

При відборі та управлінні групою з аудиту, яка має бути призначена для проведення конкретного аудиту сертифікації, орган з сертифікації повинен забезпечити належність компетентності для кожного завдання. Група повинна:

a) Мати відповідні технічні знання конкретної діяльності в межах СМІБ, щодо якої необхідна сертифікація і, де необхідно, споріднених процедур та їх потенційних ризиків щодо інформаційної безпеки (дану функцію можуть виконувати технічні експерти);
b) Мати розуміння клієнта, достатнє для проведення такого, що викликає довіру аудиту сертифікації СМІБ з огляду на сферу СМІБ та зв'язки в межах організації при управлінні аспектами інформаційної безпеки свої діяльності, продукції та послуг;
c) Мати належне розуміння законодавчих та регуляторних вимог, застосовних до СМІБ клієнта.

ПРИМІТКА Під належним розумінням не мається на увазі поглибленні знання законодавства.

9.2.3 План аудиту

Застосовуються вимоги ISO/IEC 17021-1, п. 9.2.3. Додатково застосовуються наступні вимоги та настанови.

9.2.3.1 IS 9.2.3 Загальні положення

План аудиту щодо проведення аудиту СМІБ повинен приймати до уваги визначений контроль інформаційної безпеки.

9.2.3.2 IS 9.2.3 Методи проведення аудиту за допомогою мережі

План аудиту повинен визначати методи проведення аудиту за допомогою мережі, які будуть використані під час аудиту, якщо доцільно.

Методи проведення аудиту за допомогою мережі можуть включати, наприклад, телеконференції, засідання за допомогою мережі, інтерактивне спілкування через мережу та віддалений електронний доступ до документації СМІБ або її процесів. Слід щоб такі методи зосереджувались на підвищені ефективності та продуктивності аудиту, також слід щоб вони підтримували цілісність процесу аудиту.

9.2.3.3 IS 9.2.3 Час для проведення аудиту

Слід, щоб орган з сертифікації погоджував із організацією, аудит якої буде проведено, час для аудиту, який би найкраще продемонстрував повну сферу організації. До розгляду можуть прийматися пора року, місяць, день/дати та зміни якщо належно.

9.3 Первинна сертифікація

Застосовуються вимоги ISO/IEC 17021-1, п. 9.3. Додатково застосовуються наступні вимоги та настанови.

9.3.1 IS 9.3.1 Первинний сертифікаційний аудит

9.3.1.1 IS 9.3.1.1 Етап 1

На цьому етапі аудиту орган з сертифікації повинен отримати документацію щодо проекту СМІБ, що охоплює документацію, яку вимагає ISO/IEC 27001.

Орган з сертифікації повинен отримати достатнє розуміння щодо проекту СМІБ у контексті організації-клієнта, оцінки ризиків та їх вирішення (охоплюючи визначені засоби контролю), політики і цілі щодо інформаційної безпеки і, зокрема, готовність клієнта до аудита. Зазначене дозволяє планувати етап 2.

Результати етапу 1 повинні бути задокументовані у письмовому звіті. Орган з сертифікації повинен здійснити аналіз звіту про етап 1 аудиту до прийняття рішення щодо переходу до етапу 2 та відбору групи з аудиту із необхідною компетентністю для етапу 2.

Орган з сертифікації повинен повідомити клієнта щодо можливості виникнення потреби у наданні подальшої інформації та записів для більш детального розгляду під час етапу 2.

9.3.1.2 IS 9.3.1.2 Етап 2

9.3.1.2.1 Ґрунтуючись на висновках, задокументованих у звіті щодо етапу 1 аудиту, орган з сертифікації розробляє план аудиту для здійснення етапу 2. Додатково, для оцінки ефективного впровадження СМІБ, цілями етапу 2 є:

а) що клієнт власні політики, цілі та процедури.

9.3.1.2.2 Для того щоб це зробити аудит щодо клієнта повинен зосередитись на наступному:

a) Лідерство вищого керівництва та зобов’язання щодо політики інформаційної безпеки, а також цілі щодо інформаційної безпеки;
b) Вимоги щодо документації, перелічені в ISO/IEC 27001;
c) Оцінка ризиків ~~стосовно~~ інформаційної безпеки і те, що при повторенні такі оцінки надають послідовний, дійсний та порівнювальний (порівнянний) результат;
d) Визначення цілей контролю та контролю, який ґрунтується на оцінці ризиків інформаційної безпеки та процесах зменшення ризиків;
e) Результативність інформаційної безпеки та ефективність СМІБ, оцінені відповідно до цілей щодо інформаційної безпеки;
f) Відповідність між визначеним контролем, Положенням про Застосовність і результати оцінки ризику інформаційної безпеки та процес зменшення ризику і політика щодо інформаційної безпеки та цілі;
g) Впровадження контролю (див. Додаток А), приймаючи до уваги зовнішні та внутрішні зв’язки та споріднені ризики, моніторинг за організацією, вимірювання та аналіз контролю та процесів інформаційної безпеки з метою визначення того, чи контроль впроваджено та він є ефективним і відповідає заявленим цілям щодо інформаційної безпеки;

h) Програми, процеси, процедури, записи, внутрішні аудити та аналіз ефективності СМІБ для гарантування того, що вони є простежуваними до рішень, прийнятих вищим керівництвом та політики щодо інформаційної безпеки і цілей.

9.4 Проведення аудитів

Застосовуються вимоги ISO/IEC 17021-1, п. 9.4. Додатково застосовуються наступні вимоги та настанови.

9.4.1 9.4 Загальні положення

Орган з сертифікації повинен мати задокументовані процедури щодо:

a) Первинного сертифікаційного аудиту СМІБ клієнта у відповідності до положень ISO/IEC 17021-1;
b) Наглядових аудитів та аудитів повторної сертифікації СМІБ клієнта у відповідності до ISO/IEC 17021-1 на періодичній основі для постійної відповідності вимогам та для перевірки и реєстрування того, що клієнт вчасно вживає коригувальні дії для усунення всіх невідповідностей.

9.4.2 IS 9.4 Окремі елементи аудиту СМІБ

Орган з сертифікації, який представляє група з аудиту, повинен:

a) Вимагати щоб клієнт продемонстрував відповідність та достатність оцінки ризиків щодо інформаційної безпеки функціонування СМІБ в межах її сфери;
b) Встановити чи є процедури клієнта щодо визначення, вивчення та оцінювання ризиків щодо інформаційної безпеки та результати їх впровадження відповідними до політик, цілей та задач клієнта.

Орган з сертифікації також повинен встановити чи є процедури щодо оцінки ризику чіткими та впровадженими в повній мірі.

9.4.3 IS Звіт про аудит

9.4.3.1 На додаток до вимог щодо звітності, викладених в п. 9.4.8 ISO/IEC 17021-1, звіт про аудит повинен надавати наступну інформацію або посилатися на неї:

a) Відомості про аудит, включаючи висновки щодо аналізу документів;
b) Відомості про аудит сертифікації аналізу ризику інформаційної безпеки клієнта;
c) Відхилення від плану аудиту (наприклад, більший або менший обсяг часу, витрачений на заплановані заходи);
d) Сфера СМІБ.

9.4.3.2 Звіт про аудит повинен бути деталізованим в достатній мірі для сприяння та підтримки рішення щодо сертифікації. Він повинен містити:

a) Значні досліджені сліди аудиту та використані методології аудиту (див. 9.1.3.2);
b) Зроблені спостереження, як позитивні (особливості варті зазначення), так і негативні (наприклад, потенційні невідповідності);
c) Коментарі щодо відповідності СМІБ клієнта вимогам сертифікації із чіткою заявою щодо невідповідності, посилання на версію Положення про застосовність та, якщо застосовно, будь-яке корисне порівняння із результатами попередніх аудитів сертифікації клієнта.

Заповнені анкети, чек-листи, спостереження, журнали або нотатки аудитора можуть формувати невід'ємну частину звіту про аудит. Якщо ці методи використовуються, зазначені документі повинні бути направлені до органу з сертифікації в якості доказів для підтримки рішення про сертифікацію. Інформація щодо обраних для оцінювання даних повинна бути включена до звіту про аудит або до іншої документації щодо сертиікації.

Звіт повинен розглядати достатність внутрішньої організації та процедур прийнятих клієнтом для надавання впевненості в СМІБ.

На додаток до вимог щодо звітування, викладених в п. 9.4.8 ISO/IEC 17021-1, звіт повинен охоплювати:

- підсумки щодо найбільш важливих спостережень, як позитивних, так і негативних щодо впровадження та ефективності вимог СМІБ контролю інформаційної безпеки;

- рекомендації групи з аудиту щодо того, чи слід сертифікувати СМІБ клієнта або ні, із інформацією, що підтримує таку рекомендацію.

9.5 Рішення щодо сертифікації

Застосовуються вимоги ISO/IEC 17021-1, п. 9.5. Додатково застосовуються наступні вимоги та настанови.

9.5.1 IS Рішення щодо сертифікації

Рішення щодо сертифікації повинне ґрунтуватися, на додаток до вимог ISO/IEC 17021-1, на рекомендаціях щодо сертифікації від групи з аудиту, наданих у звіті про аудит (див. 9.4.3).

Особам з комітетів, які приймають рішення щодо надання сертифікації не слід зазвичай змінювати (відхиляти) відкидати негативну рекомендацію ~~від~~ групи з аудиту. При виникненні такої ситуації, орган з сертифікації повинен задокументувати та обґрунтувати причину рішення не враховувати ~~щодо зміни~~ рекомендації.

Сертифікація не повинна надаватися клієнту до надання достатніх доказів демонстрації того, що заходи щодо аналізу керівництва та внутрішніх аудитів СМІБ є ефективними і будуть підтримуватись.

9.6 Підтримання сертифікації

9.6.1 Загальні положення

Застосовуються вимоги ISO/IEC 17021-1, п. 9.6.1.

9.6.2 Діяльність з нагляду

Застосовуються вимоги ISO/IEC 17021-1, п. 9.6.2. Додатково застосовуються наступні вимоги та настанови.

9.6.2.1 IS 9.6.2 Діяльність з нагляду

9.6.2.1.1 Процедури з наглядового аудиту повинні бути узгодженими із процедурами щодо аудиту сертифікації СМІБ клієнта як це описано в даному міжнародному стандарті.

Метою нагляду є перевірка того, що затверджена СМІБ продовжує впроваджуватись, а також розгляд внесення змін до цієї системи як результат змін в діяльності клієнта та для

підтвердження постійної відповідності вимогам сертифікації. Програми наглядового аудиту повинні охоплювати щонайменше:

a) Елементи підтримки системи, такі як оцінка ризику інформаційної безпеки та підтримка контролю, внутрішній аудит СМІБ, аналіз керівництва та коригувальні дії;
b) Зв'язок із зовнішніми зацікавленими сторонами, як того вимагає стандарт СМІБ ISO/IEC 27001 та інші документи, необхідні для сертифікації;
c) Зміни до задокументованої системи;
d) Області, які змінились;
e) Обрані вимоги ISO/IEC 27001;
f) Інші обрані належні області.

9.6.2.1.2 Під час кожного нагляду орган з сертифікації повинен проводити аналіз щонайменше наступного:

a) Ефективність СМІБ з огляду на досягнення цілей політики клієнта щодо інформаційної безпеки;
b) Функціонування процедур щодо періодичного оцінювання та аналізу відповідності із спорідненим законодавством та нормативними актами у сфері інформаційної безпеки;
c) Визначені зміни до контролю та, як результат, зміни до Положення про Застосовність;
d) Впровадження та ефективність контролю відповідно до програми аудиту.

9.6.2.1.3 Орган з сертифікації повинен бути в змозі змінювати свою програму нагляду відповідно до проблем інформаційної безпеки, які стосуються ризиків та впливу на клієнта та обґрунтувати цю програму.

Наглядові аудити можуть бути скомбіновані із аудитами інших систем менеджменту. звітність повинна чітко виділяти аспекти, що стосуються кожної системи менеджменту.

Під час наглядових аудитів органи з сертифікації повинні перевіряти записи щодо апеляцій та скарг, що надійшли до органу з сертифікації та, при встановленні будь-якої невідповідності або ~~невдачі при~~ недостатності виконання вимог сертифікації, для того, щоб впевнитися, що клієнт провів розслідування власної СМІБ та процедур і вжив необхідних коригувальних дій.

Звіт про нагляд повинен містити, зокрема, інформацію щодо усунення попередньо встановлених невідповідностей, версію Положення про застосовність та важливі зміни з часу попереднього аудиту. Звіти щодо нагляду повинні щонайменше охоплювати вимоги зазначених вище п. 9.6.2.1.1 та п. 9.6.2.1.2.

9.6.3 Повторна сертифікація

Застосовуються вимоги ISO/IEC 17021-1, п. 9.6.3. Додатково застосовуються наступні вимоги та настанови.

9.6.3.1 IS 9.6.3 Аудити повторної сертифікації

Процедури щодо аудиту повторної сертифікації повинні бути узгодженими із процедурами щодо первинного сертифікаційного аудиту СМІБ клієнта як це описано в даному міжнародному стандарті.

Час, який дається на впровадження коригувальних дій повинен бути співвідносним із тяжкістю невідповідності та спорідненого ризику щодо інформаційної безпеки.

9.6.4 Спеціальні аудити

Застосовуються вимоги ISO/IEC 17021-1, п. 9.6.4. Додатково застосовуються наступні вимоги та настанови.

9.6.4.1 IS 9.6.4 Спеціальні випадки

Діяльність, необхідна для виконання спеціальних аудитів повинна бути об'єктом спеціального провадження, якщо клієнт із сертифікованою СМІБ вносить значні зміни до своєї системи або якщо мають місце інші зміни, що може призвести до негативного впливу на основи сертифікації.

9.6.5 Тимчасове зупинення, скасування або скорочення сфери сертифікації

Застосовуються вимоги ISO/IEC 17021-1, пункт 9.6.5.

9.7 Апеляції

Застосовуються вимоги ISO/IEC 17021-1, пункт 9.7.

9.8 Скарги

Застосовуються вимоги ISO/IEC 17021-1, пункт 9.8. Додатково застосовуються наступні вимоги та настанови.

9.8.1 IS 9.8 Скарги

Скарги являють собою потенційний інцидент та позначення можливої невідповідності.

9.9 Записи щодо клієнтів

Застосовуються вимоги ISO/IEC 17021-1, пункт 9.9.

10 Вимоги щодо системи менеджменту для органів з сертифікації

10.1 Варіанти

Застосовуються вимоги ISO/IEC 17021-1, пункт 10.1. Додатково застосовуються наступні вимоги та настанови.

10.1.1 IS 10.1 Впровадження СМІБ

Рекомендується щоб органи з сертифікації впроваджували СМІБ у відповідності з ISO/IEC 27001.

10.2 Варіант А – Загальні вимоги до системи менеджменту

Застосовуються вимоги ISO/IEC 17021-1, пункт 10.2.

10.3 Варіант В – Вимоги системи менеджменту у відповідності з ISO 9001

Застосовуються вимоги ISO/IEC 17021-1, пункт 10.3.

Додаток А
(інформативний)

Знання та навички щодо аудиту та сертифікації СМІБ

А.1 Загальний огляд

Таблиця А.1 надає підсумкову інформацію щодо знань та навичок, необхідних для аудиту та сертифікації СМІБ, але є інформативним з огляду на те, що він тільки визначає області знань та навичок для конкретних функцій сертифікації.

Вимоги до компетентності для кожної функції зазначено в основному тексті цього міжнародного стандарту і наведена нижче таблиця надає посилання на конкретні вимоги.

Таблиця А.1 – Знання щодо аудиту та сертифікації СМІБ

	Функції сертифікації		
	Проведення аналізу заявки (Проведення аналізу заявки для визначення необхідної компетентності групи з аудиту, для відбору членів групи з аудиту та визначення часу аудиту)	Аналіз звітів про аудит та прийняття рішень щодо сертифікації	Проведення аудиту та керування групою з аудиту
Знання			
Термінологія менеджменту інформаційної безпеки, принципи, практики та техніка		7.1.2.4.2	7.1.2.1.2
Стандарти/нормативні документи щодо систем менеджменту інформаційної безпеки	7.1.2.3.1	7.1.2.4.3	7.1.2.1.3
Практика щодо менеджменту бізнеса			7.1.2.1.4
Бізнес сектор клієнта	7.1.2.3.2	7.1.2.4.4	7.1.2.1.5
Продукти, процеси та організація клієнта	7.1.2.3.3	7.1.2.4.5	7.1.2.1.6

А.2 Загальні положення щодо компетентності

Існує кілька шляхів, якими аудитору можуть підтвердити свої знання та досвід. Знання та досвід можливо оцінити, наприклад, при використанні визнаної кваліфікації. Реєстраційні записи щодо ~~щодо~~ схеми сертифікації персоналу також можуть бути використані для оцінювання необхідних знань та досвіду. Необхідний рівень компетентності для групи з аудиту слід встановити у відповідності з технологічною областю/ сектором організації та складністю СМІБ.

А.3 Спецальні знання та досвід

А.3.1 Типові знання щодо СМІБ

На додаток до вимог п. 7.1.2 слід розглядати наступне. Аудиторам слід мати знання та розуміння щодо наступних предметів аудиту та СМІБ:

- Складання плану та програми аудиту;
- Типів та методології аудиту;
- Ризиків аудиту;
- Аналізу процесів інформаційної безпеки;
- Безперервне поліпшення;
- Проведення внутрішнього аудиту інформаційної безпеки.

Аудиторам слід мати знання та розуміння наступних регуляторних вимог:

- Інтелектуальна власність;
- Зберігання, захист та утримання організаційних записів;
- Захист даних та приватність;
- Регулювання криптографічного контролю;
- Електронна торгівля;
- Електронні та цифрові підписи;
- Спостереження за робочім місцем;
- Перехоплення телекомунікацій та моніторинг даних (наприклад, електронної пошти);
- Зловживання в комп'ютерній сфері;
- Збір електронних доказів;
- Випробування щодо проникнень;
- Міжнародні та національні вимоги конкретного сектору (наприклад, банківська сфера).

Додаток В
(нормативний)

Час аудиту

В.1 Вступ

Даний додаток містить додаткові вимоги, які стосуються п. 9.1 ISO/IEC17021-1. Даний додаток наводить мінімальні вимоги та настанови для органу з сертифікації при розробці власних процедур для визначення кількості часу, необхідного для сертифікації сфери СМІБ клієнта різних розмірів та складності щодо широкого кола діяльності.

Органи з сертифікації повинні визначити час аудиту, який повинен витрачатися на первинну сертифікацію, нагляд та повторну сертифікацію для кожного клієнта і сертифікованої СМІБ. Використання даного додатку в період планування аудиту має результатом формування послідовного підходу до визначення належного часу аудита. В керівництві, що наведене в додатку, також враховується гнучкість по відношенню до результатів аудиту, особливо під час першого етапу, і складність сфери застосування СМІБ, що розглядається.

Даний Додаток наводить:

- Концепцію розрахунку часу аудиту (В.2);
- Вимоги щодо процедур для визначення часу аудиту для різних етапів аудиту (з В.3 по В.5);
- Вимоги щодо аудитів розгалуженої структури (В.6).

Приклади розрахунку часу аудиту щодо застосування Додатку В знаходяться у Додатку С.

Основною думкою цього підходу є те що схемі розрахунку щодо визначення часу аудиту слід:

a) Розглядати лише обґрунтовані показники, які можливо визначити;
b) Бути легкими для продуктивного застосування органами з сертифікації;
c) Нести достатній комплексний характер для повноцінного розрізнення.

Визначення часу аудиту ґрунтується на цифрах, наведених в Додатку В.1 («Таблиця часу аудиту»), що знаходиться нижче. При визначенні часу необхідно розглянути додаткові фактори для його змінення.

В.2 Підхід (Концепція)

В.2.1 Кількість персоналу, що виконує роботу під організаційним контролем

Загальна кількість персоналу, що виконує роботу під організаційним контролем у всіх змінах є початковою точкою при визначенні часу аудиту.

ПРИМІТКА Термін «персонал, що виконує роботу під організаційним контролем» є аналогом терміну «персонал» у стандарті ISO/IEC 17021-1.

Частково зайнятий персонал, що виконує роботу під організаційним контролем, додається до кількості персоналу, що виконує роботу під організаційним контролем, залежно від кількості відпрацьованих годин в порівнянні до повністю зайнятого персоналу, що виконує

роботу під організаційним контролем. Таке визначення повинно залежати від кількості відпрацьованих годин у порівнянні із повністю зайнятим співробітником.

B.2.2 День аудиту

«Час аудиту», на який посилається таблиця, зазначається у значенні «днів аудиту», витрачених на аудит. Основою розрахунку, викладеного у Додатку B є 8-ми годинний робочий день.

B.2.3 Тимчасова ділянка

Тимчасовою ділянкою є місцезнаходження, яке відрізняється від ділянок, визначених документами щодо сертифікації, і на якому на певний період часу впроваджено діяльність, що знаходиться в межах сфери сертифікації. Такі ділянки можуть різнитися від великих ділянок щодо менеджменту проектів до маленьких ділянок щодо надання послуг/монтажу. Слід щоб необхідність щодо відвідування таких ділянок та ступінь відбору ґрунтувалися на оцінюванні ризиків щодо неспроможності виконати цілі в області інформаційної безпеки через невідповідність, яка може виникнути на тимчасовій ділянці. Слід щоб обрана вибірка щодо таких ділянок представляла коло потреб щодо компетентності та варіантів послуг, що надає організація за результатами розгляду розмірів та типів діяльності, а також різних етапів проектів, що знаходяться на виконанні. Щодо загальної вибірки див. п. 9.1.5.1.

B.3 Процедура визначення часу аудиту для первинного аудиту

B.3.1 Загальні положення

Розрахунок часу аудиту повинен відповідати задокументованій процедурі.

B.3.2 Дистанційний аудит

Якщо для взаємодії із організацією використовуються дистанційні методи аудиту такі як інтерактивне співробітництво за допомогою мережі, засідання через мережу, телеконференції та/або електронна перевірка процесів організації, цю діяльність слід визначити у плані аудиту (див. 9.2.3) і може розглядатися як такий, що частково впливає на «час аудиту на місці».

Якщо орган з сертифікації розробляє план аудиту, в якому діяльність з дистанційного аудиту складає більш ніж 30% запланованого часу аудиту на місці, орган з сертифікації повинен обґрунтувати план аудиту та отримати окреме погодження від органу з акредитації перед його застосуванням.

ПРИМІТКА Під часом аудиту на місці мається на увазі час аудиту, розподілений для окремих ділянок. Електронні аудити віддалених ділянок вважаються дистанційними аудитами, навіть якщо електронні аудити фізично виконуються в приміщенні організації.

B.3.3 Розрахунок часу аудиту

Наведена нижче таблиця часу аудиту встановлює відправну точку для середньої кількості днів первинного аудиту (тут і в подальшому це число відображає дні для первинного аудиту (етап 1 та етап 2)), яка, відповідно до сталого досвіду, є належною для сфери СМІБ із зазначеною кількістю персоналу, що виконує роботу під організаційним контролем. Відповідно до сталого досвіду також відомо, що деякі зі сфер СМІБ такого ж розміру будуть потребувати дещо більше або менше часу.

Таблиця часу аудитора надає основну схему, яка може використовуватися для планування проведення аудиту шляхом визначення відправної точки, заснованої на загальній кількості співробітників всіх змін, регулювання цієї кількості на основі значущих для області аудиту щодо застосування СМІБ факторів, і додання кожному фактору свого коефіцієнта важливості (адитивний або субтрактивний) з метою визначення необхідної кількості працівників. Терміни, що використовуються в цій таблиці, пояснюються в В 2 а Додаток С надає приклади того як це можливо зробити.

Таблиця В.1 – Таблиця часу аудиту

Кількість персоналу, що виконує роботи під контролем організації	Час первинного аудиту СМЯ (дні аудиту)	Час первинного аудиту СМНС (дні аудиту)	Час первинного аудиту СМІБ (дні аудиту)	Адитивні та субтрактивні (понижуючі) фактори	Загальний час аудиту
1~10	1.5-2	2.5-3	5	Див. В.3.4	
11 ~ 15	2.5	3.5	6	Див. В.3.4	
16 ~25	3	4.5	7	Див. В.3.4	
26 ~ 45	4	5.5	8.5	Див. В.3.4	
46 ~ 65	5	6	10	Див. В.3.4	
66~85	6	7	11	Див. В.3.4	
86~125	7	8	12	Див. В.3.4	
126~175	8	9	13	Див. В.3.4	
176~275	9	10	14	Див. В.3.4	
276~425	10	11	15	Див. В.3.4	
426~625	11	12	16.5	Див. В.3.4	
626~875	12	13	17.5	Див. В.3.4	
876~1,175	13	15	18.5	Див. В.3.4	
1,176~1.550	14	16	19.5	Див. В.3.4	
1,551~2,025	15	17	21	Див. В.3.4	
2,026~2,675	16	18	22	Див. В.3.4	
2,676 ~3,450	17	19	23	Див. В.3.4	
3,451~4,350	18	20	24	Див. В.3.4	
4,351~5,450	19	21	25	Див. В.3.4	
5,451~6,800	20	23	26	Див. В.3.4	
6,801~8,500	21	25	27	Див. В.3.4	
8,501~10,700	22	27	28	Див. В.3.4	
> 10,700	та ж прогресія	та ж прогресія	та ж прогресія	Див. В.3.4	

В.3.4 Фактори для зміни часу аудиту

Таблиця часу аудиту не повинна використовуватись окремо. Розподілений час також повинен враховувати наступні фактори, що відносяться до складності СМІБ та, таким чином, до зусиль, необхідних для аудиту СМІБ:

a) Складність СМІБ (наприклад, критичність інформації, ситуації в межах СМІБ щодо ризику тощо);
b) Тип(и) діяльності, що виконується в межах сфери СМІБ;

c) Попередньо продемонстрована результативність СМІБ;
d) Ступінь та різноманітність технологій, що використовуються при впровадженні різних компонентів СМІБ (наприклад, кількість різних IT платформ, кількість відокремлених мереж);
e) Ступінь аутсорсингу та договорів із третьою стороною, що використовуються в межах сфери СМІБ;
f) Ступінь розвитку інформаційної системи;
g) Кількість звичайних ділянок та ділянок з аварійного поновлення;
h) Для наглядових аудитів та аудитів повторної сертифікації: кількість та ступінь змін, що мають відношення до СМІБ, у відповідності до п. 8.5.3 ISO/IEC 17021-1.

Додаток С надає приклади щодо того як можливо врахувати зазначені різні фактори під час розрахунку часу аудиту.

Додатковими прикладами факторів, що потребують додаткового часу аудиту є:

- Складна логістика, яка охоплює більш ніж одну будівлю або місце розташування відповідно до сфери СМІБ;
- Персонал, що розмовляє більш ніж на одній мові (потреба в перекладачі (перекладачах) або неможливість для окремих аудиторів працювати незалежно) або документація, що надається на більш ніж одній мові;
- Діяльність, що потребує відвідування тимчасових ділянок для підтвердження діяльності постійної ділянки (ділянок), система менеджменту яких є об’єктом сертифікації (див. перелік, наданий в абзаці нижче);
- Велика кількість стандартів та регуляторних актів, застосовних до СМІБ.

Прикладами факторів, що дозволяють зменшити час аудиту є:

- Продукція/процеси, що мають низький/відсутній ризик;
- Процеси, що мають єдину загальну діяльність (наприклад, тільки послуги);
- Високий процент персоналу, що здійснює роботи під контролем організації виконує однакові завдання;
- Попереднє знання організації (наприклад, якщо організація вже була сертифікована на відповідність вимогам іншого стандарту тим самим органом з сертифікації);
- Високий ступінь підготовленості клієнта до сертифікації (наприклад, вже сертифіковано або визнано іншою схемою третьої сторони);
- Високий ступінь сталості системи менеджменту на місці.

У ситуаціях, в яких клієнт сертифікації або сертифікована організація надає свою продукцію або послуги на тимчасових ділянках, важливо щоб оцінювання таких ділянок було включено сертифікаційного аудиту або програм нагляду.

Вищезазначені фактори повинні бути розглянуті та правки повинні бути внесені для тих факторів, які обґрунтовують більший або менший час аудиту для ефективного аудиту. Адитивні фактори можуть компенсуватися субтрактивними факторами. У всіх випадках, в яких внесено корективи до часу, наданого відповідно до розкладу аудиту, необхідно підтримувати достатні докази та записи для обґрунтування таких змін.

B.3.5 Обмеження щодо відхилення від часу аудиту

Для забезпечення виконання ефективних аудитів та забезпечення надійних і порівняних результатів, час аудиту, зазначений в діаграмі часу аудиту не повинен бути зменшений більш ніж на 30%.

Необхідно встановити та задокументувати відповідні причини відхилення.

B.3.6 Час аудиту на місці

Очікується, що час, розрахований разом на планування та написання звіту не буде зазвичай зменшувати загальний «час аудиту» на місці більш ніж до 70% від часу, відображеного в діаграмі часу аудиту. При потребі у додатковому часі для планування та/або написанні звіту, це не повинне бути обґрунтуванням для зменшення часу аудиту на місці. Час, який аудитор проводить у дорозі, не включається до розрахунку і додається до часу аудиту, вказаного у діаграмі.

ПРИМІТКА Значення в 70% є фактором, що ґрунтується на досвіді аудитів СМІБ.

B.4 Час аудитів для наглядових аудитів

Для циклу аудитів при первинній сертифікації, слід щоб час нагляду для даної організації був пропорційним часу, витраченому на проведення первинного аудиту і щорічно складав приблизно 1/3 часу, витраченого на проведення первинного аудиту. Запланований час нагляду слід періодично переглядати, щоб врахувати зміни, що можуть вплинути на час аудиту. Час, витрачений на наглядовий аудит повинен бути збільшений при проведенні аудиту змін в СМІБ (таких як аудит нових або змінених засобів контролю).

B.5 Час аудиту для аудиту повторної сертифікації

Загальна кількість часу, витраченого на виконання аудиту повторної сертифікації повинна залежати від результатів будь-яких попередніх аудитів, як це визначено в п. 9.4.3 даного стандарту та п. 9.6.3 ISO/IEC17021-1. Слід щоб кількість часу, витраченого на аудит повторної сертифікації була пропорційною часу, що був би витрачений на первинний сертифікаційний аудит даної організації та слід щоб він складав щонайменше 2/3 часу, який би знадобився на первинний сертифікаційний аудит даної організації на той момент часу, коли необхідно провести повторну сертифікацію.

B.6 Час аудиту при розгалуженій структурі

Кількість днів аудиту для кожної ділянки, включаючи центральний офіс, повинна розраховуватись для кожної ділянки.

Для прийняття до уваги частин аудиту, що не має відношення до центрального офісу або місцевих ділянок, можливо застосувати зменшення часу. Орган з сертифікації повинен записати причини для обґрунтування такого зменшення.

Додаток С
(інформативний)
Методи розрахунку часу аудиту

С.1 Загальні положення

Цей додаток надає подальші настанови щодо складання формули для розрахунку часу аудиту. Розділ С.2 надає приклад класифікації факторів, які можуть біти використані в якості основи для розрахунку часу аудиту, а розділ С.3 надає приклад розрахунку часу аудиту.

С.2 Класифікація факторів для розрахунку часу аудиту

Таблиця С.1 надає приклади щодо класифікації головних факторів для розрахунку часу аудиту, які перелічено в підпунктах з a) по h) розділу В.3.4. Органи з сертифікації можуть використати цю класифікацію для складання схеми розрахунку часу аудиту відповідно до п. 9.1.4.1:

Таблиця С.1 – Класифікація факторів для розрахунку часу аудиту

	Вплив на зусилля		
	Зменшені зусилля	Звичайні зусилля	Підвищені зусилля
Фактори (див. В.3.4)			
a) складність СМІБ: • Вимоги до інформаційної безпеки (конфіденційність, цілісність та доступність); • Кількість критичних активів (critical assests); • Кількість процесів та послуг.	• Невелика кількість закритої або конфіденційної інформації, низькі вимоги до доступності; • Небагато критичних ресурсів; • Лише один ключовий виробничий процес з кількома інтерфейсами та невеликою кількістю залучених виробничих підрозділів	• Вищі вимоги до доступності або деяка закрита/конфіденційна інформація; • Деякі критичні ресурси; • 2-3 простих виробничі процеси з кількома інтерфейсами та невеликою кількістю залучених виробничих підрозділів	• Велике число закритої або конфіденційної інформації (наприклад, охорона здоров'я, інформація щодо особи, страхування, банківська сфера) або високі вимоги до доступності; • Велика кількість критичних ресурсів; • Більш ніж 2 складних процеси з великою кількістю залучених інтерфейсів та виробничих підрозділів.
b) Тип(и) діяльності, що виконуються в межах сфери СМІБ	• Діяльність з низким ризиком без регуляторних вимог	• Високі регуляторні вимоги	• Високий ризик щодо діяльності з (виключно) обмеженими регуляторними вимогами
c) Попередньо продемонстрована результативність СМІБ	• Нещодавно пройшла сертифікація • Не було проведено сертифікацію, але СМІБ є повністю впровадженою, було проведено кілька аудитів та циклів поліпшення включаючи задокументовані внутрішні аудити, аналіз з боку керівництва та ефективне безперервне покращення системи	• Нещодавно пройшов наглядовий аудит	• Не проходило сертифікації та нещодавніх аудитів; • СМІБ є новою і такою, що не впроваджено в повному обсязі (наприклад, нестача окремих механізмів контролю системи менеджменту, несталі процеси постійного поліпшення, імпровізація при виконанні процесів).

d) Ступінь та різноманітність технолгій, що використовуються при впровадженні різних компонентів СМІБ (наприклад, кількість різних IT платформ, кількість відокремлених мереж)	• Високо стандартизоване середовище із невилокою різноманітністю (кілька IT платформ, серверів, операційних систем, баз даних, мереж тощо)	• Стандартизовані, але різноманітні IT платформи, сервери, операційні системи, бази даних, мережі	• Висока різноманітність або складність IT (наприклад, велика кількість різних сегментів мережі, типів серверів або баз даних, кількість ключових програм)
e) ступінь аутсорсингу та угоди із третьою стороною, що використовуються в межах сфери СМІБ	• Відсутність аутсорсингу та невеликий рівень залежності від постачальників; • Чітке визначення, менеджмент та моніторинг угод щодо аутсорсингу; • Наявність сертифікованої СМІБ у організації, що надає аутсорсинг; • Наявні відповідні незалежні звіти про страхування;	• Кілька договорів на аутсорсинг щодо яких менеджмент здійснюється частково	• Висока залежність від діяльності з аутсорсингу або постачальників із великим впливом на важливу виробничу діяльність; • Невизначений обсяг аутсорсингу, або • Кілька договорів щодо аутсорсингу щодо яких менеджмент здійснюється частково
f) ступінь розвитку системи інформаційної безпеки	• Відсутність внутрішньої розробки системи • Використання стандартизованих програмних платформ	• Використання стандартизованих програмних платформ із комплексною конфігурацією/параметрами • Високий ступінь індивідуалізації програмного забезпечення • Деякий обсяг діяльності з розробки (вмежах організації або на умовах аутсорсингу)	• Інтенсивна діяльність з внутрішньої розробки програмного забезпечення із кількома активними проектами, що мають на меті важливу виробничу ціль
g) кількість звичайних ділянок та ділянок з аварійного поновлення	• Низькі вимоги до доступності та відсутність або наявність лише однієї альтернативної ділянки з аварійного поновлення	• Середні або високі вимоги до доступності та відсутність або наявність лише однієї альтернативної ділянки з аварійного поновлення	• Високі вимоги до доступності, наприклад, цілодобові послуги • Кілька альтернативних ділянок з аварійного поновлення • Кілька центрів даних (дата-центрів)
h) для наглядового аудиту та аудиту повторної сертифікації: кількість та ступінь змін, що відносяться до СМІБ у відповідності до п. 8.5.3 ISO/IEC 17021-1	• Відсутність змін з часу останнього аудиту повторної сертифікації	• Незначні зміни у сфері або Положенні про застосовність СМІБ, наприклад, деякі політики, документи тощо	• Значні зміни у сфері або Положенні про застосовність СМІБ, наприклад, нові процеси, нові виробничі підрозділи, області, методологія менеджменту оцінки ризиків, політики, документація, зменшення ризиків • Значні зміни у вищезазначених факторах

С.3 Приклад розрахунку часу аудиту

Наступний приклад відображає як орган з сертифікації може використати фактори, викладені в розділі В.3 для розрахунку часу аудиту Розрахунок часу аудиту у приведеному нижче прикладі працює наступним чином:

Крок 1: Визначення факторів, що мають відношення до діяльності та організації (окрім ІТ середовища): визначення належного ступеню для кожної з категорій, наведених в Таблиці С.2 та складання результатів.

Крок 2: Визначення факторів, що мають відношення до ІТ середовища: визначення належного ступеню для кожної з категорій, наведених в Таблиці С.3 та складання результатів.

Крок 3: Ґрунтуючись на результатах кроків 1 та 2, зазначених вище, визначити вплив факторів на час аудиту шляхом обрання належного запису в Таблиці С.4.

Крок 4: Остаточний розрахунок: Кількість днів, визначених при застосуванні діаграми часу аудиту (Таблиця В.1) помножується на фактори, які є результатом кроку 3. Якщо використовується вибірка при розгалуженій структурі, кількість розрахованих днів аудиту збільшується залежно від зусиль, необхідних для виконання плану вибірки при розгалуженій структурі.

Такий результат є остаточною кількістю днів аудиту.

Таблиця С.2 – Фактори, що відносяться до діяльності та організації (окрім ІТ)

Категорія	Ступінь
Тип(и) вимог до діяльності та регуляторних вимог	1. Організація працює в некритичних секторах діяльності та нерегульованих секторах[a] 2. Організація має клієнтів в критичних секторах діяльності[a] 3. Організація працює в критичних секторах діяльності[a]
Процес та завдання	1. Стандартні процеси із стандартними та повторюваними завданнями; велика кількість людей здійснює роботу під контролем організації, виконуючи однакові завдання; невелика кількість продукції або послуг 2. Стандартні, але не повторювані процеси із великою кількістю продукції або послуг 3. Комплексні процеси, велика кількість продукції та послуг, велика кількість виробничих підрозділів, включених до сфери сертифікації (СМІБ охоплює процеси високої складності або відносно велике число унікальних видів діяльності)
Рівень сталості СМ	1. СМІБ вже сталою та/або впроваджено інші системи менеджменту 2. Деякі елементи інших систем менеджменту впроваджено, а якійсь – ні 3. Відсутність інших впроваджених систем менеджменту, СМІБ є новою і не є сталою
[a] Критичними секторами бізнесу є сектори, що можуть мати вплив на критичні державні служби, що призведе до ризику для здоров'я, безпеки, економіки, образ держави та її спроможність функціонувати, що може мати дуже великий негативний вплив на країну.	

Таблиця С.3 – Фактори, що мають відношення до ІТ середовища

Категорія	Ступінь
Складність ІТ інфраструктури	1. Невелика кількість або високо стандартизовані ІТ платформи, сервери, операційні системи, бази даних, мержі тощо. 2. Декілька різних ІТ платформ, серверів, операційних систем, баз даних, мереж 3. Велика кількість різних ІТ платформ, серверів, операційних систем, баз даних, мереж
Залежність від аутсорсингу та постачальників, включаючи хмарні сервіси	1. Невелика або відсутня залежність від аутсорсингу або постачальників 2. Невелика залежність від аутсорсингу або постачальників, що має відношення до деякої, але не всієї важливої виробничої діяльності 3. Велика залежність від аутсорсингу або постачальників, значний вплив на важливу виробничу діяльність
Розробка інформаційної системи	1. Відсутній або дуже обмежений обсяг внутрішньої розробки системи/програм 2. Невеликий обсяг внутрішньої або такої, що здійснюється на умовах аутсорсингу розробки системи/програм для деяких важливих виробничих цілей 3. Великий обсяг внутрішньої або такої, що здійснюється на умовах аутсорсингу розробки системи/програм для деяких важливих виробничих цілей

Таблиця С.4 – Вплив факторів на час аудиту

		Складність ІТ		
		Низька (від 3 до 4)	Середня (від 5 до 6)	Висока (від 7 до 9)
Складність бізнесу	Висока (від 7 до 9)	Від +5% до + 20%	Від +10% до +50%	Від +20% до +100%
	Середня (від 5 до 6)	Від -5% до -10%	0%	Від +10% до 50%
	Низька (від 3 до 4)	Від -10% до -30%	Від -5% до -10%	Від +5% до +20%

ПРИКЛАД 1 Організація, в якій буде проведено аудит має 700 співробітників, таким чином, відповідно до Таблиці В.1, для проведення первинного аудиту необхідно 17,5 днів. Організація не здійснює діяльність в критичному виробничому секторі, має високо стандартизовані та повторюванні завдання і нещодавно запровадила СМІБ. Відповідно до Таблиці С.2, зазначене призводить до використання фактору, який стосується виробничої діяльності ита організації та складає 1+1+3 = 5. Організація має в наявності зовсім невелику кількість ІТ платформ та баз даних, але широко використовує аутсорсинг. Організація не веде розробки як в своїх межах, так і на умовах аутсорсингу. Відповідно до Таблиці С.3, зазначене призводить до використання фактору, який стосується ІТ середовища та складає 1+3+1 = 5. Зазначене не призведе до змін в часі аудиту після використання Таблиці С.4.

ПРИКЛАД 2 Така ж сама організація як в попередньому прикладі, за винятком того, що в ній вже запроваджено декілька систем менеджменту, а СМІБ вже є сталою. Відповідно до Таблиці С.2, зазначене змінить розрахунок таким чином: 1+1+1 = 3. Відповідно до Таблиці С.4, зазначене призведе до зменшення часу аудиту на 5-10%, тобто час аудиту буде зменшено на 1-1.5 днів і він загалом складатиме від 16 до 16.5 днів.

Додаток D
(інформативний)
Настанови щодо аналізу впровадженого стандарту ISO/IEC 27001:2013, засобів контролю Додатку А

D.1 Мета

Впровадження засобів контролю, що були визначені клієнтом як необхідні для СМІБ (відповідно до Положення про застосовність), повинні бути проаналізовані протягом етапу 2 первинного аудиту та протягом здійснення діяльності з нагляду або повторної сертифікації (див. 9.3.1.2.2 g)).

Докази аудиту, що збираються органом з сертифікації, повинні бути достатніми для формування висновку щодо ефективності засобів контролю. Запланований результат від засобу контролю, наприклад, може бути вказаним в процедурах або політиках клієнта.

D.1.1 Докази аудиту

Найкращі докази аудиту збираються шляхом спостережень, зроблених аудитором (наприклад, двері, щ повинні бути зачиненими зачинено, угоди про конфіденційність підписано, реєстр активів існує та містить помічені активи, системні налаштування є належними тощо). Докази можливо зібрати при розгляді результативності засобу контролю (наприклад, папери з правами доступу, надані персоналу, підписано уповноваженою посадовою особою, записи щодо резолюцій за інцидентами, оформлення повноважень підписано відповідною уповноваженою посадовою особою, протоколи засідань керівництва (або інших засідань) тощо). Докази можуть бути результатом безпосередніх випробувань аудитором (або повторних результатів) засобів контролю, наприклад, спроби виконати завдання, заборонені засобами контролю, з'ясування чи встановлено на машинах останні версії програмного забезпечення для захисту від шкідливого коду, надано права доступу (після узгодження із уповноваженими особами) тощо. Докази можливо збирати шляхом співбесід з особами, що здійснюють діяльність під контролем організації/субпідрядниками щодо процесів ті засобів контролю та визначення того, чи їх твердження фактично відповідають дійсності.

D.2 Як використовувати Таблицю D.1

D.2.1 Загальні положення

Таблиця D.1 надає настанови для аналізу впровадження засобів контролю, перелічених в Додатку А до ISO/IEC 27001:2013, та для збору доказів аудиту щодо їх результативності під час первинного та наступних аудитів. Метою таблиці не є надання настанов щодо аналізу засобів контролю, що відрізняються від перелічених в Додатку А до ISO/IEC 27001:2013.

D.2.2 Колонки «Організаційний контроль» та «Технічний контроль»

«Х» у відповідній колонці відображає чи є засіб контролю організаційним або технічним. З огляду на те, що деякі засоби контролю є одночасно організаційними та технічними, позначки можуть міститися в обох колонках таких контролів.

Докази результативності організаційних засобів контролю можуть бути зібрані шляхом аналізу записів щодо результативності засобів контролю, співбесід, спостережень та фізичної перевірки. Докази щодо результативності технічних засобів контролю можуть

зазвичай бути зібрані шляхом випробувань системи (див. нижче) або шляхом використання спеціалізованих інструментів щодо аудиту/звітування.

D.2.3 Колонка «Випробування системи»

«Випробування системи» означає безпосередній аналіз інформаційних систем (наприклад, аналіз системних налаштувань або конфігурації). Знайти відповіді на питання аудитора можливо в системній консолі або шляхом оцінювання результатів інструментів випробувань. Якщо клієнт використовує відомий аудитору комп'ютерний інструмент, це може бути використано для підтримки аудиту або для аналізу результатів оцінювання, виконаного клієнтом (або його субпідрядниками).

Таблиця містить дві категорії щодо аналізу технічних засобів контролю:

– «можливо»: випробування системи є можливим для оцінювання впровадження засобів контролю, але може бути необов'язковим при аудиті СМІБ;

– «рекомендовано»: випробування системи зазвичай є необхідним при аудиті СМІБ.

ПРИМІТКА В межах даного Додатку «система» означає «інформаційну систему» якщо не вказано інше.

D.2.4 Колонка «Візуальна перевірка»

«Візуальна перевірка» означає, що дані засоби контролю зазвичай вимагають візуальної перевірки на місці для оцінювання їх ефективності. Це означає, що аналіз відповідної документації на паперовому носії або співбесіда не є достатніми; аудитору слід перевірити засіб контролю на місці його впровадження.

D.2.5 Колонка «Настанови щодо аналізу під час аудиту»

Колонка «Настанови щодо аналізу під час аудиту» надає можливі напрямки роботи для оцінювання засобів контролю в якості подальших настанов для аудитора.

Таблиця D.1 – Класифікація засобів контролю

Засоби контролю відповідно до Додатку А ISO/IEC 27001:2013	Організаційні засоби контролю	Технічні засоби контролю	Випробування системи	Візуальна перевірка	Настанови щодо аналізу під час аудиту
A.5 Політики щодо інформаційної безпеки					
A.5.1 Вказівки керівництва щодо інформаційної безпеки					
A.5.1.1 Політики щодо інформаційної безпеки	X				
A.5.1.2 Аналіз політик щодо інформаційної безпеки	X				
A.6 Організація інформаційної безпеки					

A.6.1 Внутрішня організація					
A.6.1.1 Ролі та відповідальність щодо інформаційної безпеки	X				
A.6.1.2 Розподілення обов'язків	X				
A.6.1.3 Зв'язок із владою	X				
A.6.1.4 Зв'язок із зацікавленими групами	X				
A.6.1.5 Інформаційна безпека щодо менеджменту проектів	X				
A.6.2 Мобільні пристрої та віддалена робота					
A.6.2.1 Політика щодо мобільних пристроїв	X	X	можливо		Також перевірити впровадження політики де це застосовно
A.6.2.2 Віддалена робота	X	X	можливо		Також перевірити впровадження політики де це застосовно
A.7 Безпека людських ресурсів					
A.7.1 Перед працевлаштуванням					
A.7.1.1 Відбір	X				
A.7.1.2 Норми та умови працевлаштування	X				
A.7.2 Протягом працевлаштування					
A.7.2.1 Менеджмент відповідальності	X				
A.7.2.2 Обізнаність, освіта та навчання щодо інформаційної безпеки	X				Запитати персонал чи вони обізнані стосовно конкретних речей, щодо яких вони повинні мати знання
A.7.2.3 Дисциплінарний процес	X				
A.7.3 Припинення та зміни щодо працевлаштування					
A.7.3.1 Відповідальність щодо припинення або змін в працевлаштуванні	X				
A.8 Менеджмент активів					

A.8.1 Відповідальність за активи					
A.8.1.1 Інвентар Перелік активів	X				Визначення активів
A.8.1.2 Права власності на активи	X				
A.8.1.3 Прийнятне використання активів	X				
A.8.1.4 Повернення активів	X				
A.8.2 Класифікація інформації					
A.8.2.1 Класифікація інформації	X				Також перевірити впровадження політики де це застосовно
A.8.2.2 Позначення інформації	X				Назви: директорій, файлів, роздрукованих звітів, записаних медіа (наприклад, касети, диски, CD), електронні повідомлення та переміщення файлів
A.8.2.3 Поводження з активами	X				
A.8.3 Поводження із носіями					
A.8.3.1 Менеджмент змінних носіїв	X	X	МОЖЛИВО		
A.8.3.2 Зняття носіїв з експлуатації	X			X	Процес зняття з експлуатації
A.8.3.3 Фізичне переміщення носіїв	X				Фізичний захист
A.9 Контроль доступу					
A.9.1.1 Політика контролю доступу	X				Також перевірити впровадження політики де це застосовно
A.9.1.2 Доступ до мереж та мережеві послуги	X				Також перевірити впровадження політики де це застосовно
A.9.2 Менеджмент доступу користувачів					
A.9.2.1 Реєстрація та видалення користувачів	X				
A.9.2.2 Надання доступу користувачам	X	X	МОЖЛИВО		Вибірково перевірити персонал, що виконує роботу під контролем організації /субпідрядників

					щодо повноважень на права доступ до всіх систем
A.9.2.3 Менеджмент привілейованих прав доступу	X	X	можливо		Внутрішнє переміщення персоналу
A.9.2.4 Менеджмент секретної інформації користувачів щодо входу	X				
A.9.2.5 Аналіз прав доступу користувачів	X				
A.9.2.6 Видалення або змінення прав доступу	X				
A.9.3 Відповідальність користувачів					
A.9.3.1 Використання секретної інформації щодо входу	X				Перевірити наявність настанов/політики для користувачів
A.9.4 Управління доступом до системи та програм					
A.9.4.1 Обмеження доступу до інформації	X	X	рекомендовано		
A.9.4.2 Процедури безпечного входу	X	X	рекомендовано		
A.9.4.3 Система менеджменту паролів	X	X	рекомендовано		
A.9.4.4 Використання привілейованих допоміжних програм	X	X	рекомендовано		
A.9.4.5 Контроль доступу до вихідного коду програм	X	X	рекомендовано		
A.10 Криптографія					
A.10.1 Криптографічний контроль					
A.10.1.1 Політика щодо використання криптографічних засобів управління	X				Також перевірити впровадження політики де це застосовно
A.10.1.2 Менеджмент ключів	X	X	рекомендовано		Також перевірити впровадження політики де це застосовно
A.11 Фізична безпека та безпека навколишнього середовища					
A.11.1 Безпечні зони					

A.11.1.1 Фізично захищений периметр	X				
A.11.1.2 Фізичні засоби управління входом (або записами???)	X	X	можливо		Архівування записів щодо входу
A.11.1.3 Забезпечення безпечності в офісах, кімнатах та будівлях	X				
A.11.1.4 Захист від зовнішніх загроз та загроз навколишнього середовища	X				
A.11.1.5 Робота у безпечних зонах	X				
A.11.1.6 Зони доставки та завантаження	X				
A.11.2 Обладнання					
A.11.2.1 Розміщення та захист обладнання	X				
A.11.2.2 Додаткові службові програми	X	X	можливо		
A.11.2.3 Безпека кабельних з'єднань	X				
A.11.2.4 Обслуговування обладнання	X				
A.11.2.5 Видалення активів	X				Записи щодо видалених активів
A.11.2.6 Безпека обладнання та активів поза приміщенням	X	X	можливо		Шифрування портативних пристроїв
A.11.2.7 Безпечне списання або повторне використання обладнання	X	X	можливо		Затирання дисків, шифрування дисків
A.11.2.8 Автономне користувацьке обладнання	X				Перевірити наявність настанов/політики для користувачів
A.11.2.9 Політика чистого стола та екрана	X				Також перевірити впровадження політики де це застосовно
A.12 Операційна безпека					
A.12.1 Операційні процедури та відповідальність					
A.12.1.1 Задокументовані операційні процедури	X				

A.12.1.2 Менеджмент змін	X	X	рекомендовано		
A.12.1.3 Менеджмент виробничої здатності	X	X	можливо		
A.12.1.4 Відокремлення середовищ розробки, випробування та оперування	X	X	можливо		
A.12.2 Захист від шкідливих програм					
A.12.2.1 Засоби управління проти шкідливих програм	X	X	рекомендовано		Конфігурація та повнота охоплення програмного забезпечення щодо контролю шкідливих програм
A.12.3 Резервне копіювання					
A.12.3.1 Резервне копіювання інформації	X	X	рекомендовано		Політика аналізу, випробування резервного копіювання
A.12.4 Ведення журналів та моніторинг					
A.12.4.1 Ведення журналів щодо подій	X	X	можливо		Обрання подій з журналу, ґрунтуючись на ризику
A.12.4.2 Захист інформації в журналах	X	X	можливо		
A.12.4.3 Журнали адміністратора та оператора	X	X	можливо		
A.12.4.4 Синхронізація годинників		X	можливо		
A.12.5 Управління операційним програмним забезпеченням					
A.12.5.1 Встановлення програмного забезпечення в операційних системах	X	X	можливо		
A.12.6 Менеджмент технічних вразливостей					
A.12.6.1 Менеджмент технічних вразливостей	X	X	рекомендовано		Менеджмент виправлень, що ґрунтується на ризиках та посиленні

					операційних систем, баз даних та програм
A.12.6.2 Обмеження щодо встановлення програмного забезпечення	X	X	можливо		
A.12.7 Положення щодо аудиту інформаційних систем					
A.12.7.1 Засоби управління аудитами інформаційних систем	X				
A.13 Безпека зв'язку					
A.13.1 Менеджмент безпеки мережі					
A.13.1.1 Засоби управління мережею	X	X	можливо		Мережевий менеджмент
A.13.1.2 Безпека мережевих послуг	X	X	рекомендовано		SLA, надання послуг з інформаційної безпеки в мережі (наприклад, VPN, маршрутизація мережі та засоби управління з'єднаннями, конфігурація мережевих пристроїв)
A.13.1.3 Розділення мереж	X	X	можливо		Діаграми мережі, сегменти мережі (наприклад, DMZ) та розділення (наприклад, VLAN)
A.13.2 Перенесення інформації					
A.13.2.1 Політики та процедури перенесення інформації	X				Також перевірити впровадження політики де це застосовно
A.13.2.2 Угоди щодо перенесення інформації	X				
A.13.2.3 Електронні повідомлення	X	X	можливо		Підтвердити, що зразки повідомлень відповідають політиці/процедурам
A.13.2.4 Угоди про конфіденційність та нерозголошення	X				Аналіз контракту
A.14 Придбання, розробка та обслуговування системи					
A.14.1 Вимоги до безпеки					

інформаційних систем					
A.14.1.1 Аналіз та специфікація вимог до інформаційної безпеки	X				
A.14.1.2 Забезпечення безпеки програмних послуг у громадських мережах	X	X	рекомендовано		Проектування програмних послуг, що ґрунтується на ризиках
A.14.1.3 Захист транзакцій через програмні послуги	X	X	рекомендовано		Конфіденційність, цілісність, виконання зобов'язань
A.14.2 Безпека процесів розробки та підтримки					
A.14.2.1 Політика щодо безпечної розробки	X				Також перевірити впровадження політики де це застосовно
A.14.2.2 Процедури контролю змін системи	X	X	рекомендовано		
A.14.2.3 Технічний аналіз програм після змін до операційної платформи	X				
A.14.2.4 Обмеження щодо змін до пакетів програмного забезпечення	X				
A.14.2.5 Принципи безпечної побудови системи	X				
A.14.2.6 Безпечне середовище розробки	X	X	можливо		
A.14.2.7 Розробка на умовах аутсорсингу	X				
A.14.2.8 Випробування безпеки системи	X				
A.14.2.9 Випробування прийнятності системи	X	X	можливо		
A.14.3 Дані випробувань					
A.14.3.1 Захист даних випробувань	X	X	можливо	X	
A.15 Відносини із постачальниками					
A.15.1 Інформаційна безпека у відношеннях із постачальниками					

A.15.1.1 Політика інформаційної безпеки щодо відносин із постачальниками	X				Також перевірити впровадження політики де це застосовно
A.15.1.2 Питання безпеки в угодах із постачальниками	X				Випробувати деякі умови контракту
A.15.1.3 Ланцюг постачання інформаційних та комунікаційних технологій	X				Випробувати деякі умови контракту
A.15.2 Менеджмент надання послуг постачальників					
A.15.2.1 Моніторинг та аналіз послуг постачальників	X				
A.15.2.2 Менеджмент змін у послугах постачальників	X				
A.16 Менеджмент інцидентів щодо інформаційної безпеки					
A.16.1 Менеджмент інцидентів та поліпшень інформаційної безпеки					
A.16.1.1 Відповідальність та процедури	X				
A.16.1.2 Звітування щодо подій, які стосуються інформаційної безпеки	X				
A.16.1.3 Звітування щодо слабких місць в інформаційній безпеці	X				
A.16.1.4 оцінка та рішення щодо подій, які стосуються інформаційної безпеки	X				
A.16.1.5 Реагування на інциденти щодо інформаційної безпеки	X				
A.16.1.6 Набуття знань за результатами інцидентів щодо інформаційної безпеки	X				

A.16.1.7 Збирання доказів	X				
A.17 Аспекти інформаційної безпеки щодо менеджменту безперервності виробничої діяльності					
A.17.1 Сталість Безперервність інформаційної безпеки					Протокол аналізу керівництва
A.17.1.1 Планування щодо сталості інформаційної безпеки	X				
A.17.1.2 Впровадження сталості інформаційної безпеки	X				
A.17.1.3 Перевірка, аналіз та оцінювання сталості інформаційної безпеки	X				
A.17.2 Скорочення (надлишок ?) Надмірність					
A.17.2.1 Доступність ресурсів щодо обробки інформації	X	X	можливо		
A.18 Відповідність					
A.18.1 Відповідність законодавчим та договірним вимогам					
A.18.1.1 Визначення застосовних законодавчих та договірних вимог	X		рекомендовано		
A.18.1.2 Права інтелектуальної власності	X				
A.18.1.3 Захист записів	X	X	рекомендовано		
A.18.1.4 Конфіденційність та захист інформації, що містить відомості про особистість	X				Також перевірити впровадження політики де це застосовно
A.18.1.5 Регулювання криптографічних засобів управління	X				
A.18.2 Аналіз інформаційної безпеки					

A.18.2.1 Незалежний аналіз інформаційної безпеки	X				Прочитати звіти
A.18.2.2 Відповідність із політиками та стандартами безпеки	X				
A.18.2.3 Аналіз технічної відповідності	X	X			