НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології

МЕТОДИ ЗАХИСТУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Вимоги

(ISO/IEC 27001:2013; Cor 1:2014, IDT)

ДСТУ ISO/IEC 27001:2015

Видання офіційне

Київ
ДП «УкрНДНЦ»
2016

ПЕРЕДМОВА

1 ВНЕСЕНО: Технічний комітет стандартизації «Інформаційні технології» (ТК 20) за участю Технічного комітету стандартизації «Банківські та фінансові системи і технології (ТК 105), Міжнародний науково-навчальний центр інформаційних технологій та систем НАН України та Міносвіти і науки України

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **І. Івченко,** канд. фіз.-мат. наук; **М. Карнаух; Т. Тищенко**

2 НАДАНО ЧИННОСТІ: наказ ДП «УкрНДНЦ» від 18 грудня 2015 р. № 193 з 2017–01–01

3 Національний стандарт відповідає ISO/IEC 27001:2013; Cor 1:2014, IDT) Information technology — Security techniques — Information security management systems — Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги)

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської (en)

4 НА ЗАМІНУ ДСТУ ISO/IEC 27001:2010

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей національний стандарт є переклад ISO/IEC 27001:2015 Information technology — Security techniques — Information security management systems — Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги) зі зміною Cor. 1:2014.

Технічний комітет стандартизації, відповідальний за цей стандарт в Україні, — ТК 105 «Банківські та фінансові системи і технології».

У цьому національному стандарті зазначено вимоги, які відповідають законодавству України.

До цього стандарту внесено такі редакційні зміни:

— слова «цей міжнародний стандарт», «ISO/IEC 27001», «цей документ» замінено на «цей стандарт»;

— вилучено «Передмову» до ISO/IEC 27001:2014 як таку, що безпосередньо не стосується тематики цього стандарту;

— структурні елементи стандарту: «Титульний аркуш», «Передмову», «Національний вступ», першу сторінку, «Терміни та визначення понять» і «Бібліографічні дані» — оформлено згідно з вимогами національної стандартизації України;

— у розділах 2 «Нормативні посилання» та «Бібліографія» наведено «Національні пояснення», в А.7.1 та А.8.1.2 — «Національні примітки», виділені рамкою;

— долучено довідковий національний додаток НА (Перелік національних стандартів України, ідентичних з міжнародними стандартами, посилання на які є в цьому стандарті).

У цьому стандарті є посилання на такий міжнародний стандарт:

ISO/IEC 27000, який прийнято як ДСТУ ISO/IEC 27000:2015 Системи управління інформаційною безпекою. Огляд і словник (IDT).

Додаток А — обов'язковий і є невід'ємною частиною цього стандарту.

Копії нормативних документів, на які є посилання в цьому стандарті, можна отримати в Національному фонді нормативних документів.

0 ВСТУП

0.1 Загальні положення

Цей стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття системи управління інформаційною безпекою є стратегічним рішенням для організації. На проектування та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги щодо безпеки, застосовувані організаційні процеси, розмір і структура організації. Очікують, що всі ці чинники змінюються з часом.

Система управління інформаційною безпекою забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам, що ризиками належним чином управляють.

Важливо, щоб система управління інформаційною безпекою була частиною та інтегрувалася в процеси організації та загальну структуру управління, щоб інформаційну безпеку розглядали в процесах розроблення, інформаційних системах і заходах безпеки. Очікують, що впровадження системи управління інформаційною безпекою буде масштабованим відповідно до потреб організації.

Цей стандарт може бути використано зацікавленими внутрішніми та зовнішніми сторонами для оцінки можливості організації відповідати власним вимогам щодо інформаційної безпеки.

Послідовність, з якою вимоги надано в цьому стандарті, не відображає їх важливості чи послідовності, з якою їх має бути впроваджено. Перелік пунктів понумеровано лише для цілей забезпечення посилань.

ISO/IEC 27000 надає огляд і словник систем управління інформаційною безпекою з посиланням на сімейство стандартів щодо систем управління інформаційною безпекою (охоплюючи ISO/IEC 27003 [2], ISO/IEC 27004 [3] та ISO/IEC 27005 [4]), з пов'язаними термінами та визначеннями.

0.2 Сумісність з іншими стандартами систем управління

Цей стандарт використовує високорівневу структуру, ідентичні назви підрозділів, ідентичний текст, загальні терміни та основні визначення, які надано в додатку SL ISO/IEC Directives, Part 1, Consolidated ISO Supplement, тому підтримує сумісність з іншими стандартами систем управління, які визначено в додатку SL.

Такий загальний підхід, визначений в додатку SL, буде корисним тим організаціям, що обирають застосування одній системі управління, яка забезпечує виконання вимог двох або більше стандартів систем управління.

Код УКНД 35.040

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги
(ISO/IEC 27001:2013; Cor 1:2014, IDT)

Місце поправки	Надруковано	Має бути
С. V, абзац 1, рядок 1	ISO/IEC 27001:2015	ISO/IEC 27001:2013

(ІПС № 10–2016)

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

МЕТОДИ ЗАХИСТУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Вимоги

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

МЕТОДЫ ЗАЩИТЫ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Требования

INFORMATION TECHNOLOGY

SECURITY TECHNIQUES INFORMATION SECURITY MANAGEMENT SYSTEMS

Requirements

Чинний від 2017–01–01

1 СФЕРА ЗАСТОСУВАННЯ

Цей стандарт визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації. Цей стандарт також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації. Вимоги, наведені в цьому стандарті, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи. Вилучення будь-якої з вимог, наведених в розділах 4—10 неприпустимо в разі, якщо організація прагне відповідати цьому стандарту.

2 НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче нормативні документи в цілому або в частині необхідні для застосування цього стандарту. У разі датованих посилань застосовують лише наведені видання. У разі недатованих посилань потрібно користуватись останнім виданням нормативних документів (разом зі змінами).

ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO/IEC 27000 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд та словник.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті використовують терміни та визначення, які надано в ISO/IEC 27000.

4 ОБСТАВИНИ ОРГАНІЗАЦІЇ

4.1 Розуміння організації та її обставин

Організація повинна визначити внутрішні та зовнішні обставини, які важливі для її цілей та впливають на можливість досягнення наперед запланованого результату(-ів) її системи управління інформаційною безпекою.

Примітка. Визначення цих обставин стосується визначення внутрішнього та зовнішнього середовища організації, розглянутого в розділі 5 3 ISO 31000:2009 [5].

4.2 Розуміння потреб та очікувань зацікавлених сторін

Організація повинна визначити:

a) зацікавлені сторони, які важливі для системи управління інформаційною безпекою; та

b) вимоги цих зацікавлених сторін, важливих для інформаційної безпеки.

Примітка. Вимоги зацікавлених сторін можуть охоплювати законодавчі та регуляторні вимоги, а також контрактні зобов'язання.

4.3 Визначення сфери застосування системи управління інформаційною безпекою

Організація повинна визначити межі та можливість застосування системи управління інформаційною безпекою для встановлення її сфери застосування.

Для визначення сфери застосування організація повинна розглянути:

a) зовнішні та внутрішні обставини, зазначені в 4.1;

b) вимоги, зазначені в 4.2; та

c) інтерфейси та залежності між діями, які виконує організація, і тими, що виконують інші організації.

Сфера застосування має бути доступною як документована інформація.

4.4 Система управління інформаційною безпекою

Організація повинна розробити, впровадити, підтримувати та постійно вдосконалювати систему інформаційної безпеки відповідно до вимог цього стандарту.

5 КЕРІВНИЦТВО

5.1 Керівництво та зобов'язання

Вище керівництво повинно продемонструвати дії з управління та зобов'язання по відношенню до систем управління інформаційною безпекою:

a) гарантуванням, що політика інформаційної безпеки та цілі інформаційної безпеки розроблені та сумісні зі стратегічними планами організації;

b) гарантуванням інтеграції вимог системи інформаційної безпеки в процеси організації;

c) гарантуванням, що ресурси, потрібні для системи управління інформаційною безпекою, доступні;

d) доведенням до відома організації важливості ефективного управління інформаційною безпекою та відповідності вимогам системи управління інформаційною безпекою;

e) гарантуванням, що система управління інформаційною безпекою досягне своїх запланованих результатів;

f) призначенням та підтримкою осіб для досягнення ефективності системи управління інформаційною безпекою;

g) сприянням постійному вдосконаленню; та

h) підтримкою інших пов'язаних ролей вищого керівництва, щоб продемонструвати їх керівну роль, яку вони застосовують у сферах їх відповідальності.

5.2 Політика

Вище керівництво повинно запровадити політику інформаційної безпеки, яка:

a) відповідає цілям організації;

b) містить цілі інформаційної безпеки (див. 6.2) або зазначає основні положення для визначення цілей інформаційної безпеки;

c) містить зобов'язання відповідати застосованим вимогам, пов'язаним з інформаційною безпекою; та

d) містить зобов'язання щодо постійного вдосконалення системи управління інформаційною безпекою.

Політика інформаційної безпеки має:

e) бути доступною як документована інформація;

f) бути розповсюдженою в середині організації; і

g) бути доступною зацікавленим сторонам, за потреби.

5.3 Організаційні ролі, відповідальності та повноваження

Вище керівництво повинно гарантувати, що відповідальності та повноваження для ролей, пов'язаних з інформаційною безпекою, призначені й доведені.

Вище керівництво повинно призначити відповідальності та повноваження для:

a) гарантування, що система управління інформаційною безпекою відповідає вимогам цього стандарту; і

b) звітування вищому керівництву щодо результативності системи управління інформаційною безпекою.

Примітка. Вище керівництво може також призначити відповідальності та повноваження для звітування щодо результативності системи управління інформаційною безпекою в межах організації.

6 ПЛАНУВАННЯ

6.1 Дії щодо ризиків та можливостей

6.1.1 *Загальні положення*

Під час планування системи управління інформаційною безпекою організація повинна розглянути питання, описані в 4.1, і вимоги, описані в 4.2, а також визначити ризики та можливості, які потрібно мати на увазі, щоб:

a) гарантувати, що система управління інформаційною безпекою може досягти запланованого результату(-ів);

b) запобігти або зменшити небажані ефекти; і

c) досягти постійного вдосконалення.

Організація повинна планувати:

d) дії, які стосуються цих ризиків та можливостей; і

e) як саме

1) інтегрувати й упровадити ці дії до процесів її системи управління інформаційною безпекою; та

2) оцінювати ефективність цих дій.

6.1.2 *Оцінка ризиків інформаційної безпеки*

Організація повинна визначити та застосовувати процес оцінювання ризиків інформаційної безпеки, який:

a) встановлює та підтримує критерії ризиків інформаційної безпеки, які містять:

1) критерії прийняття ризиків; і

2) критерії для виконання оцінки ризиків інформаційної безпеки;

b) гарантує, що повторні оцінки ризиків інформаційної безпеки призводять до послідовних, дійових та порівняльних результатів;

c) ідентифікує ризики інформаційної безпеки:

1) застосовує процес оцінювання ризиків інформаційної безпеки для ідентифікації ризиків, пов'язаних із втратою конфіденційності, цілісності й доступності в межах сфери застосування системи управління інформаційною безпекою; та

2) ідентифікує власників ризиків;

d) виконує аналіз ризиків інформаційної безпеки:

1) оцінює потенційні наслідки, які будуть результатом реалізації ризиків, ідентифікованих в 6.1.2 c) 1);

2) оцінює практичну імовірність появи ризиків, ідентифікованих у 6.1.2 c) 1); та

3) визначає рівні ризиків;

e) оцінює ризики інформаційної безпеки:

1) порівнює результати аналізу ризиків з критеріями ризиків, визначеними в 6.1.2 a); та

2) визначає пріоритети проаналізованих ризиків для оброблення ризиків.

Організація повинна зберігати документовану інформацію стосовно процесу оцінювання ризиків інформаційної безпеки.

6.1.3 *Оброблення ризиків інформаційної безпеки*

Організація повинна визначити та застосовувати процес оброблення ризиків інформаційної безпеки для:

a) вибору доречних опцій оброблення ризиків інформаційної безпеки з урахуванням результатів оцінки ризиків;

b) визначити всі заходи безпеки, які необхідно впровадити для вибраної(-их) опції(-ій) оброблення ризиків;

Примітка. Організація може розробити необхідні заходи безпеки або ідентифікувати їх з будь-якого джерела.

c) порівняти заходи безпеки, визначені в 6.1.3 b) вище, з наведеними в додатку A, і підтвердити, що не було опущено потрібних заходів безпеки;

Примітка 1. Додаток A містить всебічний перелік цілей заходів безпеки та заходів безпеки. Користувачів цього стандарту відсилаємо до додатка A для впевненості, що необхідні заходи безпеки не було пропущено.

Примітка 2. Цілі заходів безпеки повністю долучено до вибраних заходів безпеки. Перелік цілей заходів безпеки та заходи безпеки, надані в додатку A не є вичерпними і можуть бути потрібні додаткові цілі заходів безпеки та заходи безпеки.

d) підготувати Положення щодо застосовності, яке містить:

— необхідні заходи безпеки (див. 6.1.3 b) та c));

— обґрунтування для їх застосування;

— впроваджені необхідні заходи безпеки чи ні;

— обґрунтування для виключень заходів безпеки, наданих у додатку A;

e) розробити план оброблення ризиків інформаційної безпеки; та

f) отримати від власників ризиків підтвердження плану оброблення ризиків інформаційної безпеки та згоду на залишкові ризики інформаційної безпеки.

Організація повинна зберігати задокументовану інформацію щодо процесу оброблення ризиків інформаційної безпеки.

Примітка. Процес оцінювання та оброблення ризиків інформаційної безпеки в цьому стандарті відповідає принципам та загальним настановам, зазначеним в ISO 31000 [5].

6.2 Цілі інформаційної безпеки та планування їх досягнення

Організація повинна встановити цілі інформаційної безпеки для відповідних функцій та рівнів.

Цілі інформаційної безпеки мають:

a) відповідати політиці інформаційної безпеки;

b) бути вимірюваними (якщо доцільно);

c) враховувати вимоги до інформаційної безпеки, які застосовують, а також результати оцінювання ризиків та оброблення ризиків;

d) бути розповсюдженими; та

e) оновлюватися, за потреби.

Організація повинна зберігати документовану інформацію щодо цілей інформаційної безпеки.

Під час планування дій для досягнення цілей інформаційної безпеки організація повинна визначити:

f) що треба зробити;

g) які ресурси будуть потрібні;

h) хто буде відповідальним;

i) коли процес буде завершено; та

j) як результати будуть оцінювати.

7 ПІДТРИМКА

7.1 Ресурси

Організація повинна визначити й забезпечувати наявність ресурсів, потрібних для розроблення, впровадження, підтримання й постійного вдосконалення системи управління інформаційною безпекою.

7.2 Компетенція

Організація повинна:

a) визначити рівень необхідної компетентності персоналу, який виконує роботи, що впливають на результативність інформаційної безпеки;

b) гарантувати, що цей персонал має компетенцію на основі відповідного навчання, тренінгів або досвіду;

c) за можливості, забезпечувати виконання певних дій для досягнення необхідної компетенції та оцінювати ефективність таких дій; і

d) зберігати відповідну документовану інформацію як доказ компетентності.

Примітка. Можливі дії можуть охоплювати, наприклад: проведення тренінгів, наставництво або перепризначення наявних працівників, або наймання на роботу чи за контрактом компетентних осіб.

7.3 Обізнаність

Персонал, який виконує функції під наглядом організації, повинен бути обізнаним в:

a) політиці інформаційної безпеки;

b) його вкладі в ефективність системи управління інформаційною безпекою, враховуючи переваги від вдосконалення результативності інформаційної безпеки; та

c) розумінні невідповідності вимогам системи управління інформаційною безпекою.

7.4 Комунікація

Організація повинна визначити потребу у внутрішніх та зовнішніх комунікаціях з питань системи управління інформаційною безпекою, включаючи:

a) з яких питань спілкуватися;

b) коли спілкуватися;

c) з ким спілкуватися;

d) хто повинен спілкуватися; та

e) процеси, за допомогою яких комунікація повинна відбуватися.

7.5 Документована інформація

7.5.1 *Загальні положення*

Система управління інформаційною безпекою організації повинна включати:

a) документовану інформацію, визначену цим стандартом; і

b) документовану інформацію, визначену організацією як необхідну для ефективності системи управління інформаційною безпекою.

Примітка. Обсяги документованої інформації для системи управління інформаційною безпекою можуть бути різними для різних організацій залежно від:

1) розміру організації й типу її діяльності, процесів, продуктів і послуг;
2) складності процесів та їх взаємодії; і
3) компетенції персоналу.

7.5.2 *Створення та оновлення*

У разі створення й оновлення документованої інформації організація повинна гарантувати відповідну:

a) ідентифікацію та опис (наприклад, назву, дату, автора чи посилальний номер);

b) формат (наприклад, мову, версію програмного забезпечення, графіки) та носії (наприклад, папір, електронні); та

c) перегляд і затвердження для відповідності й адекватності.

7.5.3 *Контроль документованої інформації*

Задокументована інформація, визначена системою управління інформаційною безпекою та цим стандартом має контролювати для гарантії того, що:

a) вона доступна й придатна для використання, де і коли вона потрібна; і

b) її належним чином захищено (наприклад, від втрати конфіденційності, помилкового використання або втрати цілісності).

Для контролю документованої інформації організація повинна виконувати такі дії відповідним чином:

c) розподіл, доступ, повернення та використання;

d) збереження та консервування, зокрема й консервування чіткості/розбірливості;

e) контроль змін (наприклад, контроль версій); та

f) утримування й розташування.

Документована інформація від зовнішнього джерела, визначена організацією як необхідна для планування та функціонування системи управління інформаційною безпекою, має бути ідентифікована відповідних чином і контрольована.

Примітка. Доступ означає рішення стосовно дозволу лише на перегляд документованої інформації чи дозволу та повноважень на перегляд і зміну документованої інформації тощо.

8 ФУНКЦІОНУВАННЯ

8.1 Робоче планування й контроль

Організація повинна планувати, впроваджувати й контролювати процеси, необхідні для виконання вимог інформаційної безпеки, а також впроваджувати дії, визначені в 6.1. Організація також повинна впроваджувати плани для досягнення цілей інформаційної безпеки, визначених в 6.2.

Організація повинна зберігати документовану інформацію в обсязі, необхідному для впевненості, що процес виконується як було заплановано.

Організація повинна контролювати заплановані зміни та переглядати наслідки непередбачених змін, застосовуючи дії для усунення будь-яких шкідливих дій, за потреби.

Організація повинна гарантувати, що процеси, віддані на аутсорсинг, визначені й контрольовані.

8.2 Оцінювання ризиків інформаційної безпеки

Організація повинна виконувати оцінювання ризиків через заплановані інтервали або коли запропоновані чи відбуваються суттєві зміни з урахуванням критеріїв, визначених в 6.1.2 a).

Організація повинна зберігати задокументовану інформацію стосовно результатів оцінювання ризиків інформаційної безпеки.

8.3 Оброблення ризиків інформаційної безпеки

Організація повинна впровадити план оброблення ризиків інформаційної безпеки.

Організація повинна зберігати задокументовану інформацію стосовно результатів оброблення ризиків інформаційної безпеки.

9 ОЦІНЮВАННЯ РЕЗУЛЬТАТИВНОСТІ

9.1 Моніторинг, вимірювання, аналіз та оцінювання

Організація повинна оцінювати результативність інформаційної безпеки та ефективність системи управління інформаційною безпекою.

Організація повинна визначити:

a) що саме потрібно моніторити й вимірювати, включаючи процеси інформаційної безпеки та заходи безпеки;

b) методи моніторингу, вимірювань, аналізу та оцінювання, які може бути застосовано для гарантії обґрунтованих результатів;

Примітка. Обрані методи, які надають порівняні та відтворювані результати, можна розглядати як обґрунтовані.

c) коли моніторинг та вимірювання потрібно виконувати;

d) хто повинен виконувати моніторинг та вимірювання;

e) коли результати моніторингу та вимірювань потрібно аналізувати й оцінювати; та

f) хто повинен аналізувати й оцінювати ці результати.

Організація повинна зберігати відповідну задокументовану інформацію як доказ результатів моніторингу та вимірювань.

9.2 Внутрішній аудит

Організація повинна проводити внутрішні аудити через заплановані інтервали часу для забезпечення того, що інформація чи система управління інформаційною безпекою:

a) відповідають

1) власним вимогам організації для її системи управління інформаційною безпекою; та

2) вимогам цього стандарту;

b) ефективно впроваджена та підтримується.

Організація повинна:

c) планувати, розробляти, впроваджувати та підтримувати програму(-и) аудиту, зокрема й частоту, методи, відповідальності, заплановані вимоги та звітність. Програма(-и) аудиту повинна(-і) враховувати аналіз важливості процесів, що їх розглядають, і результати попередніх аудитів;

d) визначити критерії аудиту та сферу застосування для кожного аудиту;

e) призначити аудиторів і виконати аудити, які гарантують об'єктивність і неупередженість процесу аудиту;

f) гарантувати, що результати аудиту буде доведено до відповідного керівництва; та

g) зберігати документовану інформацію як доказ програми аудиту та результатів аудиту.

9.3 Перегляд з боку керівництва

Вище керівництво повинно переглядати систему управління інформаційною безпекою організації через заплановані проміжки часу для гарантування її постійної придатності, адекватності й ефективності.

Перегляд з боку керівництва повинен стосуватися розгляду:

a) статусу дії, що є наслідком попереднього перегляду керівництва;

b) зміни в зовнішніх та внутрішніх обставинах, які мають відношення до системи управління інформаційною безпекою;

c) зворотного впливу на результативність інформаційної безпеки, охоплюючи тенденції в:

1) невідповідностях та коригувальних діях;

2) результатах моніторингу та вимірювань;

3) результатах аудиту; та

4) досягненнях цілей інформаційної безпеки;

d) зворотного зв'язку від зацікавлених сторін;

e) результатів оцінювання ризиків і статусу плану оброблення ризиків; та

f) можливостей для постійного вдосконалення.

Вихідні дані перегляду з боку керівництва повинні включати рішення стосовно можливостей постійного вдосконалення та будь-яких потреб внесення змін до системи управління інформаційною безпекою.

Організація повинна зберігати документовану інформацію як доказ результатів переглядів з боку керівництва.

10 ВДОСКОНАЛЕННЯ

10.1 Невідповідності й корегувальні дії

У разі виявлення невідповідностей організація повинна:

a) реагувати на невідповідності і за можливості:

1) виконувати дії для контролю та їх корекції; та

2) вживати заходів щодо наслідків;

b) оцінювати потреби в діях для усунення причин невідповідностей для запобігання їх повторення чи виникнення будь-де за допомогою:

1) перегляду невідповідностей;

2) визначення причин невідповідностей; і

3) визначення, чи існують подібні невідповідності або потенційно можуть з'являтися;

c) впровадити певні дії, за потреби;

d) переглянути ефективність виконаних коригувальних дій; і

e) внести зміни до системи управління інформаційною безпекою, за потреби.

Коригувальні дії мають бути адекватними до наслідків виявлених невідповідностей.

Організація повинна зберігати документовану інформацію як доказ:

f) сутності невідповідностей та будь-яких послідовних дій, що були виконані, та

g) результати будь-яких коригувальних дій.

10.2 Постійне вдосконалення

Організація повинна постійно вдосконалювати придатність, адекватність та ефективність системи управління інформаційною безпекою, гарантування її постійної придатності, адекватності та ефективності.

ДОДАТОК А
(обов'язковий)

ЦІЛІ ЗАХОДІВ БЕЗПЕКИ ТА ЗАХОДИ БЕЗПЕКИ

Цілі заходів безпеки та заходи безпеки, наведені в таблиці А.1, безпосередньо виведені та узгоджені з тих цілей заходів безпеки та заходів безпеки, наведених в ISO/IEC 27002:2013 [1], розділи 5—18, і мають використовуватися в контексті розділу 6.1.3.

Таблиця А.1 — Цілі заходів безпеки та заходи безпеки

А.5 Політики безпеки		
А.5.1 Принципи управління інформаційною безпекою		
Ціль: Забезпечити принципи управління та підтримку інформаційної безпеки згідно з вимогами бізнесу та відповідними законами й нормативами.		
А.5.1.1	Політики інформаційної безпеки	Заходи безпеки Набір політик щодо інформаційної безпеки повинен бути визначений, затверджений керівництвом, виданий і доведений до відома всього найманого персоналу та потрібних зовнішніх сторін
А.5.1.2	Перегляд політики інформаційної безпеки	Заходи безпеки Політики інформаційної безпеки потрібно переглядати в заплановані інтервали часу або за появи істотних змін для забезпечення їх постійної придатності, адекватності й ефективності
А.6 Організація інформаційної безпеки		
А.6.1 Внутрішня організація		
Ціль: Визначити структуру управління для започаткування та контролю впровадження та функціонування інформаційної безпеки в організації.		
А.6.1.1	Ролі та обов'язки щодо інформаційної безпеки	Заходи безпеки Усі обов'язки щодо інформаційної безпеки необхідно чітко визначити та розподілити
А.6.1.2	Розподіл обов'язків	Заходи безпеки Конфліктуючі обов'язки та сфери відповідальності мають бути розподілені для зменшення можливостей неавторизованої чи ненавмисної модифікації або неправильного використання ресурсів СУІБ організації
А.6.1.3	Контакти з повноважними органами	Заходи безпеки Необхідно підтримувати належні контакти з відповідними повноважними органами
А.6.1.4	Контакти з групами фахівців з певної проблематики	Заходи безпеки Необхідно підтримувати належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об'єднаннями
А.6.1.5	Інформаційна безпека в управлінні проектами	Заходи безпеки Інформаційну безпеку потрібно брати до уваги під час управління проектами незалежно від типу проекту

A.6.2 Мобільне обладнання та віддалена робота		
Ціль: Гарантувати безпеку віддаленої роботи та використання мобільного обладнання.		
A.6.2.1	Політика щодо мобільного обладнання	Заходи безпеки Політика та заходи підтримання безпеки мають бути пристосовані до управління ризиками, які виникають за рахунок використання мобільного обладнання
A.6.2.2	Віддалена робота	Заходи безпеки Політика та заходи підтримання безпеки мають бути запроваджені для захисту інформації, яка доступна, обробляється чи зберігається в місцях віддаленої роботи
A.7 Безпека людських ресурсів		
A.7.1 Перед наймом **Національна примітка** Слово «найм» тут призначене, щоб охопити всі різноманітні ситуації: наймання людей (тимчасове чи постійне), призначення на посади, зміну посад, підписання контрактів та припинення дії будь-якої з цих угод.		
Ціль: Гарантувати, що найманий персонал та підрядники розуміють свої обов'язки, придатні до ролей, на які претендують.		
A.7.1.1	Ретельна перевірка	Заходи безпеки Підтверджувальні перевірки біографічних даних усіх кандидатів на найм мають виконуватись згідно з усіма відповідними законами, нормативами та морально-етичними нормами, а також співвідносно до бізнес-вимог, класифікації інформації, до якої потрібен доступ, і усвідомлюваних ризиків
A.7.1.2	Терміни та умови найму	Заходи безпеки Контрактна угода з найманим персоналом та підрядниками має встановити взаємні відповідальності щодо інформаційної безпеки
A.7.2 Протягом найму		
Ціль: Впевнитися, що весь найманий персонал та підрядники усвідомлюють і виконують свої обов'язки з інформаційної безпеки.		
A.7.2.1	Відповідальність керівництва	Заходи безпеки Керівництво повинно вимагати від найманого персоналу та підрядників застосування заходів безпеки згідно з установленими в організації політиками та процедурами
A.7.2.2	Поінформованість, освіта й навчання щодо інформаційної безпеки	Заходи безпеки Увесь найманий персонал організації, а там, де це суттєво, і підрядники повинні одержати належне навчання й тренінги для поінформованості та регулярно отримувати оновлені дані щодо політик і процедур організації, суттєвих для їх посадових функцій
A.7.2.3	Дисциплінарний процес	Заходи безпеки Має існувати формальний та офіційно оформлений дисциплінарний процес щодо найманого персоналу, який порушив інформаційну безпеку

A.7.3 Припинення чи зміна умов найму		
Ціль: Захистити інтереси організації як частини процесу зміни умов чи припинення найму.		
A.7.3.1	Припинення чи зміна відповідальностей	Заходи безпеки Має бути чітко визначено, доведено до найманого персоналу чи підрядників і встановлено відповідальності за інформаційну безпеку та обов'язки, які залишаються дійсними після припинення чи зміни умов найму
A.8 Управління ресурсами СУІБ		
A.8.1 Відповідальність за ресурси СУІБ		
Ціль: Ідентифікувати ресурси СУІБ організації і визначити відповідні обов'язки щодо їх захисту		
A.8.1.1	Інвентаризація ресурсів СУІБ	Заходи безпеки Інформація, ресурси СУІБ, пов'язані з інформацією та обладнанням для обробки інформації, мають бути ідентифіковані та має підтримуватися їх актуальний інвентарний опис
A.8.1.2	Володіння ресурсами СУІБ	Заходи безпеки Ресурси СУІБ, які наявні в інвентарному описі, мають «бути у власності».
Національна примітка Термін «власник» ідентифікує особу чи організацію, для якої встановлено затверджену керівництвом відповідальність щодо контролювання виробництва, розвитку, підтримування, використання та безпеки ресурсів СУІБ. Термін «власник» не означає, що особа дійсно має право власності на ресурс СУІБ.		
A.8.1.3	Припустиме використання ресурсів СУІБ	Заходи безпеки Правила щодо припустимого використання інформації та ресурсів СУІБ, пов'язаних із засобами оброблення інформації, мають бути ідентифіковані, задокументовані та впроваджені
A.8.1.4	Повернення ресурсів СУІБ	Заходи безпеки Увесь найманий персонал та користувачі зовнішньої сторони повинні повернути всі ресурси СУІБ організації, що перебувають у їх володінні, після припинення їх найму, контракту чи угоди
A.8.2 Класифікація інформації		
Ціль: Забезпечити належний рівень захисту інформації відповідно до її важливості для організації.		
A.8.2.1	Класифікація інформації	Заходи безпеки Інформація має бути класифікована в термінах правових вимог, її цінності, критичності й чутливості для неавторизованого розкриття чи модифікації
A.8.2.2	Маркування інформації	Заходи безпеки Має бути розроблено та впроваджено належну множину процедур для маркування й оброблення інформації згідно зі схемою класифікації, прийнятою організацією
A.8.2.3	Поводження з ресурсами СУІБ	Заходи безпеки Має бути розроблено та впроваджено процедури поводження з ресурсами СУІБ відповідно до схеми класифікації інформації, яку офіційно прийнято в організації

A.8.3 Поводження з носіями		
Ціль: Запобігти несанкціонованому розголошенню, модифікації, вилученню або знищенню інформації, яка зберігається на носіях.		
A.8.3.1	Управління змінними носіями	Заходи безпеки Має бути впроваджено процедури управління змінними носіями відповідно до схеми класифікації, запровадженої в організації
A.8.3.2	Вилучення носіїв	Заходи безпеки Коли носії більше не потрібні, їх треба безпечно вилучати із застосуванням офіційно оформлених процедур
A.8.3.3	Фізичні носії під час передавання	Заходи безпеки Носії, що містять інформацію, має бути захищено від несанкціонованого доступу, зловживання чи руйнування під час транспортування
A.9 Контроль доступу		
A.9.1 Бізнес-вимоги до контролю доступу		
Ціль: Обмежити доступ до інформації та засобів оброблення інформації.		
A.9.1.1	Політика контролю доступу	Заходи безпеки Політика контролю доступу має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та інформаційної безпеки
A.9.1.2	Доступ до мереж та послуг мережі	Заходи безпеки Користувачі повинні отримувати доступ до мережі та послуг мережі лише тоді, коли вони були спеціально авторизовані для використання
A.9.2 Управління доступом користувача		
Ціль: Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг.		
A.9.2.1	Реєстрація та зняття з реєстрації користувача	Заходи безпеки Має бути впроваджено процес реєстрації та зняття з реєстрації для того, щоб була можливість управляти правами доступу
A.9.2.2	Забезпечення доступу користувачів	Заходи безпеки Має бути впроваджено формально затверджений процес забезпечення доступу користувачу для надання або вилучення прав доступу для всіх типів користувачів до всіх систем та послуг
A.9.2.3	Управління привілейованими правами доступу	Заходи безпеки Призначення та використання привілейованих прав доступу має бути обмежено та контрольовано
A.9.2.4	Управління таємною інформацією автентифікації користувачів	Заходи безпеки Облік таємної інформації автентифікації користувачів потрібно контролювати за допомогою офіційно оформленого процесу управління
A.9.2.5	Перегляд прав доступу користувача	Заходи безпеки Власники ресурсів СУІБ повинні переглядати права доступу користувача через регулярні встановлені інтервали

A.9.2.6	Вилучення або корекція прав доступу	Заходи безпеки Права доступу всього найманого персоналу та користувачів зовнішніх сторін до інформації та засобів оброблення інформації мають вилучатися після припинення найму, контракту чи угоди, або коректуватися після змін
A.9.3 Відповідальності користувача		
Ціль: Зробити користувачів відповідальними за збереження їх інформації автентифікації.		
A.9.3.1	Використання таємної інформації автентифікації	Заходи безпеки Треба вимагати від користувачів додержання визначених в організації практик у використанні таємної інформації автентифікації
A.9.4 Контроль доступу до систем та прикладних програм		
Ціль: Запобігти несанкціонованому доступу до систем та прикладних програм.		
A.9.4.1	Обмеження доступу до інформації	Заходи безпеки Доступ до інформації та функцій прикладних систем має бути обмежений відповідно до визначеної політики контролю доступу
A.9.4.2	Процедури безпечного підключення (log-on)	Заходи безпеки Доступ до систем та прикладних програм повинен контролювати процедурою безпечного підключення, коли це визначено політикою контролю доступу
A.9.4.3	Система управління паролем	Заходи безпеки Системи для управління паролями мають бути інтерактивними і забезпечувати якісні паролі
A.9.4.4	Використання привілейованих системних утиліт	Заходи безпеки Використання програм утиліт, що можуть бути спроможні скасовувати заходи безпеки системи та прикладних програм, має бути обмежено та суворо контрольовано
A.9.4.5	Контроль доступу до початкових кодів програм	Заходи безпеки Доступ до початкових кодів програм має бути обмежений
A.10 Криптографія		
A.10.1 Криптографічні засоби захисту		
Ціль: Гарантувати відповідне та ефективне використання криптографії для захисту конфіденційності, автентичності та/або цілісності.		
A.10.1.1	Політика використання криптографічних засобів	Заходи безпеки Має бути розроблено та впроваджено політику використання криптографічних засобів для захисту інформації
A.10.1.2	Управління ключами	Заходи безпеки Має бути розроблено та впроваджено політику використання, захисту й часу життя криптографічних ключів для всього їх життєвого циклу

A.11 Фізична безпека та безпека інфраструктури		
A.11.1 Зони безпеки		
Ціль: Запобігти несанкціонованому фізичному доступу, пошкодженню та втручанню в її інформацію та засоби оброблення інформації.		
A.11.1.1	Периметр фізичної безпеки	Заходи безпеки Для захисту зон, що містять конфіденційну або критичну інформацію чи засоби оброблення інформації, треба визначити та використовувати периметри безпеки
A.11.1.2	Заходи безпеки фізичного прибуття	Заходи безпеки Зони безпеки має бути захищено належними заходами безпеки прибуття, щоб гарантувати, що доступ дозволений лише персоналу, який отримав санкцію
A.11.1.3	Убезпечення офісів, кімнат та обладнання	Заходи безпеки Має бути розроблено й застосовано фізичну безпеку офісів, кімнат та обладнання
A.11.1.4	Захист від зовнішніх та інфраструктурних загроз	Заходи безпеки Має бути розроблено й застосовано фізичний захист від пошкодження внаслідок природних катаклізмів, акцій громадської непокори та аварій
A.11.1.5	Робота в зонах безпеки	Заходи безпеки Має бути розроблено та застосовано процедури роботи в зонах безпеки
A.11.1.6	Зони доставки та відвантаження	Заходи безпеки Щоб уникнути несанкціонованого доступу, має бути контрольовано й, за можливості, ізольовано від засобів оброблення інформації точки доступу, такі як зони доставки та відвантаження, а також інші точки, через які особи, доступ яких не санкціоновано, можуть увійти до службових приміщень
A.11.2 Обладнання		
Ціль: Запобігти втратам, пошкодженню, крадіжці або компрометації ресурсів СУІБ та перериванню діяльності організації.		
A.11.2.1	Розміщення та захист обладнання	Заходи безпеки Обладнання має бути розміщено чи захищено так, щоб зменшити ризики інфраструктурних загроз і небезпек та можливого несанкціонованого доступу
A.11.2.2	Допоміжні комунальні служби	Заходи безпеки Обладнання має бути захищено від аварійних відімкнень живлення та інших порушень, внаслідок аварій засобів життєзабезпечення
A.11.2.3	Безпека кабельних мереж	Заходи безпеки Силові та телекомунікаційні кабельні мережі передачі даних або підтримки інформаційних послуг має бути захищено від перехоплювання, взаємного впливу чи пошкоджень

A.11.2.4	Обслуговування обладнання	Заходи безпеки Обладнання трібно правильно обслуговувати, щоб забезпечити його постійну доступність і цілісність
A.11.2.5	Переміщення майна	Заходи безпеки Обладнання, інформацію чи програмне забезпечення не потрібно виносити назовні без попередньої санкції на ці дії
A.11.2.6	Безпека обладнання та ресурсів СУІБ поза службовими приміщеннями	Заходи безпеки До ресурсів СУІБ поза службовими приміщеннями має бути застосовний захист з урахуванням різних ризиків роботи поза службовими приміщеннями організації
A.11.2.7	Безпечне вилучення або повторне використання обладнання	Заходи безпеки Всі елементи обладнання, які містять носії пам'яті, має бути перевірено для забезпечення того, що будь-які конфіденційні дані або ліцензійне програмне забезпечення було видалено чи безпечним чином перезаписано до вилучення або повторного використання
A.11.2.8	Обладнання користувачів, залишене без нагляду	Заходи безпеки Користувачі мають забезпечити, що залишене без нагляду обладнання, належним чином захищене
A.11.2.9	Політика чистого стола та чистого екрана	Заходи безпеки Повинні бути ухвалені політика чистого стола щодо паперів і змінних носіїв інформації та політика чистого екрана щодо засобів оброблення інформації
A.12 Безпека експлуатації		
A.12. 1 Процедури експлуатації та відповідальності		
Ціль: Забезпечити коректне та безпечне функціонування засобів оброблення інформації.		
A.12.1.1	Документовані процедури експлуатації	Заходи безпеки Процедури експлуатації має бути задокументовано та зроблено доступними для всіх користувачів, що їх потребують
A.12.1.2	Управління змінами	Заходи безпеки Зміни в організації, бізнес-процесах, засобах оброблення інформації та системах, які впливають на інформаційну безпеку, мають бути контрольованими
A.12.1.3	Управління потужністю	Заходи безпеки Для забезпечення потрібної продуктивності системи необхідно здійснювати моніторинг та регулювати використання ресурсів і проектувати вимоги до майбутньої потужності
A.12.1.4	Відокремлення засобів розробки, тестування та експлуатації	Заходи безпеки Засоби розроблення, тестування та експлуатації має бути відокремлено для зменшення ризиків несанкціонованого доступу чи змін в операційному середовищі

A.12.2 Захист від зловмисного коду

Ціль: Гарантувати, що інформація та засоби оброблення інформації захищені від зловмисного коду.		
A.12.2.1	Заходи безпеки проти зловмисного коду	Заходи безпеки Має бути впроваджено заходи безпеки щодо виявлення, запобігання та відновлення для захисту від зловмисного коду і належні процедури поінформування користувачів
A.12.3 Резервне копіювання		
Ціль: Захистити від втрати даних.		
A.12.3.1	Резервне копіювання інформації	Заходи безпеки Згідно із затвердженою політикою резервного копіювання треба регулярно робити і в подальшому тестувати резервні копії інформації, програмного забезпечення та образів систем
A.12.4 Ведення журналів аудиту та моніторинг		
Ціль: Записувати події та генерувати докази.		
A.12.4.1	Журнал аудиту подій	Заходи безпеки Журнал аудиту подій, у якому записується діяльність користувачів, винятки, збої та події інформаційної безпеки, треба вести, зберігати й регулярно переглядати
A.12.4.2	Захист інформації журналів реєстрації	Заходи безпеки Засоби реєстрування та інформація реєстрації має бути захищено від фальсифікації та несанкціонованого доступу
A.12.4.3	Журнали реєстрації адміністратора та оператора	Заходи безпеки Діяльність системного адміністратора та системного оператора має реєструватися і журнали аудиту мають бути захищені та регулярно переглядатися
A.12.4.4	Синхронізація годинників	Заходи безпеки Годинники всіх важливих систем оброблення інформації в організації або домені безпеки має бути синхронізовано з джерелом часу погодженої точності
A.12.5 Контроль програмного забезпечення, що перебуває в експлуатації		
Ціль: Гарантувати цілісність систем, що перебувають в експлуатації.		
A.12.5.1	Інсталяція програмного забезпечення в системах, що перебувають в експлуатації	Заходи безпеки Мають бути наявними процедури контролю інсталяції програмного забезпечення в системах, що перебувають в експлуатації
A.12.6 Управління технічною вразливістю		
Ціль: Запобігати використанню технічних вразливостей.		
A.12.6.1	Управління технічною вразливістю	Заходи безпеки Треба отримувати своєчасну інформацію щодо технічних вразливостей інформаційних систем, які використовують, оцінювати підвладність організації таким вразливостям і вживати належних заходів, щоб урахувати пов'язаний з цим ризик

A.12.6.2	Обмеження на інсталяцію програмного забезпечення	Заходи безпеки Має бути розроблено та впроваджено правила стосовно інсталяції програмного забезпечення користувачами
A.12.7 Розгляд аудиту інформаційних систем		
Ціль: Мінімізувати вплив аудиту на системи, які перебувають у промисловій експлуатації.		
A.12.7.1	Заходи безпеки аудиту інформаційних систем	Заходи безпеки Вимоги аудиту та діяльність, що охоплює перевірки систем, які перебувають в експлуатації, має бути ретельно сплановано та погоджено, щоб мінімізувати ризик порушення бізнес-процесів
A.13 Безпека комунікацій		
A.13.1 Управління безпекою мережі		
Ціль: Забезпечити захист інформації в мережах та захист засобів оброблення інформації, що їх підтримує.		
A.13.1.1	Заходи безпеки мережі	Заходи безпеки Треба відповідним чином управляти й захищати мережі для захисту інформації в системах і прикладних програмах
A.13.1.2	Безпека послуг мережі	Заходи безпеки Характеристики безпеки, рівні послуг, а також вимоги управління всіма послугами мережі має бути ідентифіковано і міститися в будь-якій угоді щодо послуг мережі як для послуг, які надає сама організація, так і для аутсорсингових послуг
A.13.1.3	Сегментація в мережах	Заходи безпеки У мережі мають бути сегментовані групи інформаційних послуг, користувачів, а також інформаційні системи
A.13.2 Обмін інформацією		
Ціль: Підтримувати безпеку інформації, якою обмінюються всередині організації та з зовнішнім об'єктом.		
A.13.2.1	Політики та процедури обміну інформацією	Заходи безпеки Мають бути наявними офіційно оформлені політики, процедури та заходи безпеки для захисту обміну інформацією з використанням усіх видів засобів комунікації
A.13.2.2	Угоди щодо обміну інформацією	Заходи безпеки Між організацією та зовнішніми сторонами повинні бути укладені угоди щодо безпечного обміну бізнес-інформацією
A.13.2.3	Електронний обмін повідомленнями	Заходи безпеки Інформація, яка міститься в електронних повідомленнях, має бути захищена належним чином
A.13.2.4	Угоди щодо конфіденційності або нерозголошення	Заходи безпеки Вимоги до угод щодо конфіденційності або нерозголошення, які відображують потреби організації в захисті інформації, мають бути ідентифіковані, задокументовані та регулярно переглядатися

A.14 Придбання, розроблення та підтримка інформаційних систем		
A.14.1 Вимоги щодо безпеки для інформаційних систем		
Ціль: Гарантувати, що безпека є невід'ємною частиною інформаційних систем протягом всього життєвого циклу. Це також включає вимоги для інформаційних систем, які забезпечують надання послуг з використанням публічних (загальнодоступних) мереж.		
A.14.1.1	Аналіз та специфікація вимог інформаційної безпеки	Заходи безпеки Вимоги щодо інформаційної безпеки має бути долучено в положення щодо бізнес-вимог до нових інформаційних систем або модернізацій до наявних інформаційних систем
A.14.1.2	Безпечні прикладні сервіси в публічних мережах	Заходи безпеки Інформація в прикладних сервісах, яку передають через публічні мережі, має бути захищеною від шахрайської діяльності, контрактних суперечок, несанкціонованого розголошення та модифікації
A.14.1.3	Захист транзакцій прикладних сервісів	Заходи безпеки Інформація, залучена в транзакції прикладних сервісів, має бути захищена для запобігання неповній передачі, неправильній маршрутизації, несанкціонованій зміні повідомлення, несанкціонованому розголошенню, несанкціонованому дублюванню повідомлення чи його повторенню
A.14.2 Безпека в процесах розроблення та підтримки		
Ціль: Гарантувати, що інформаційну безпеку проектують та впроваджують протягом життєвого циклу розроблення інформаційних систем.		
A.14.2.1	Політика безпечного розроблення	Заходи безпеки Потрібно встановлювати та застосовувати до розробників всередині організації правила для розроблення програмного забезпечення та систем
A.14.2.2	Процедури контролю змін системи	Заходи безпеки Зміни в системах всередині життєвого циклу розроблення мають бути контрольованими за допомогою офіційно оформлених процедур контролю змін
A.14.2.3	Технічний перегляд прикладних програм після змін операційної платформи	Заходи безпеки Коли операційні платформи змінено, критичні для бізнесу прикладні програми має бути переглянуто й протестовано, щоб забезпечити відсутність негативного впливу на функціонування та безпеку організації
A.14.2.4	Обмеження на зміни до пакетів програмного забезпечення	Заходи безпеки Модифікації пакетів програмного забезпечення не повинні заохочуватися, бути обмеженими найнеобхіднішими змінами і всі зміни потрібно суворо контролювати
A.14.2.5	Принципи проектування безпечної системи	Заходи безпеки Принципи проектування безпечних систем потрібно розробити, задокументувати, виконувати та використовувати для будь-яких зусиль щодо реалізації інформаційних систем
A.14.2.6	Безпечне середовище розроблення	Заходи безпеки Організації повинні запровадити та відповідним чином захистити безпечне середовище проектування для розроблення систем та інтеграції зусиль, що покривають повний життєвий цикл розроблення системи

A.14.2.7	Аутсорсингове розроблення	Заходи безпеки Організація повинна здійснювати нагляд над аутсорсинговим розробленням систем та його моніторинг
A.14.2.8	Тестування безпеки системи	Заходи безпеки Тестування функціональності безпеки потрібно виконувати протягом розроблення
A.14.2.9	Приймальне тестування системи	Заходи безпеки Програми приймального тестування та відповідні критерії має бути визначено для нових інформаційних систем, оновлень та нових версій
A.14.3 Дані для тестування системи		
Ціль: Забезпечити захист даних, які використовують для тестування.		
A.14.3.1	Захист даних для тестування системи	Заходи безпеки Дані для тестування має бути ретельно відібрано, захищено та контрольовано
A.15 Взаємовідносини з постачальниками		
A.15.1 Інформаційна безпека у взаємовідносинах з постачальниками		
Ціль: Гарантувати захист ресурсів СУІБ організації, які можуть бути доступні постачальникам.		
A.15.1.1	Політика інформаційної безпеки для взаємовідносин з постачальниками	Заходи безпеки Вимоги інформаційної безпеки для послаблення ризиків, пов'язаних із доступом постачальників до ресурсів СУІБ організації має бути погоджено з постачальником та задокументовано
A.15.1.2	Врахування безпеки в угодах з постачальниками	Заходи безпеки Усі відповідні вимоги щодо інформаційної безпеки має бути встановлено та погоджено з кожним постачальником, який може мати доступ, обробляти, зберігати, передавати чи надавати компоненти IT-інфраструктури для інформації організації
A.15.1.3	Ланцюг постачання інформаційних та комунікаційних технологій	Заходи безпеки Угоди з постачальниками мають містити вимоги стосовно адресації ризиків інформаційної безпеки, пов'язаних з ланцюгом постачання продуктів та послуг інформаційних і комунікаційних технологій
A.15.2 Управління наданням послуг постачальником		
Ціль: Підтримувати належний рівень інформаційної безпеки та надання послуг відповідно до угод з постачальниками.		
A.15.2.1	Моніторинг та перегляд послуг постачальника	Заходи безпеки Організація повинна регулярно проводити моніторинг, перегляд та аудит отримання послуг постачальника
A.15.2.2	Управління змінами у послугах постачальника	Заходи безпеки Зміни в наданні послуг постачальника, зокрема й підтримування та вдосконалювання наявних політик інформаційної безпеки, процедур і заходів безпеки, мають управлятися з урахуванням критичності залучених бізнес-систем і процесів та переоцінки ризиків

A.16 Управління інцидентами інформаційної безпеки		
A.16.1 Управління інцидентами інформаційної безпеки та вдосконаленням		
Ціль: Гарантувати послідовний та ефективний підхід до управління інцидентами інформаційної безпеки, охоплюючи поширення інформації про події безпеки та слабкі місця.		
A.16.1.1	Відповідальності та процедури	Заходи безпеки Має бути визначено відповідальності керівництва та процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки
A.16.1.2	Звітування про події інформаційної безпеки	Заходи безпеки Необхідно якнайшвидше звітувати стосовно подій інформаційної безпеки через належні канали управління
A.16.1.3	Звітування щодо слабких місць інформаційної безпеки	Заходи безпеки Треба вимагати від усього найманого персоналу та підрядників, які користуються інформаційними системами та послугами, звертати увагу та звітувати щодо будь-яких спостережених або очікуваних слабких місць у системах чи послугах
A.16.1.4	Оцінювання та прийняття рішення стосовно подій інформаційної безпеки	Заходи безпеки Події інформаційної безпеки має бути оцінено та прийнято рішення стосовно віднесення їх до інцидентів інформаційної безпеки
A.16.1.5	Реагування на інциденти інформаційної безпеки	Заходи безпеки Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до задокументованої процедури
A.16.1.6	Знання з вивчення інцидентів інформаційної безпеки	Заходи безпеки Знання, отримані з аналізу та розв'язання інцидентів інформаційної безпеки, мають використовуватися для зменшення ймовірності чи впливу майбутніх інцидентів
A.16.1.7	Збирання доказів	Заходи безпеки Організація повинна визначити і використовувати процедури для ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як докази
A.17 Аспекти інформаційної безпеки управління безперервністю бізнесу		
A.17.1 Безперервність інформаційної безпеки		
Ціль: Безперервність інформаційної безпеки має бути залучено в системи управління безперервністю бізнесу організації.		
A.17.1.1	Планування безперервності інформаційної безпеки	Заходи безпеки Організація повинна визначити свої вимоги щодо інформаційної безпеки та безперервності управління інформаційною безпекою в надзвичайних ситуаціях, наприклад під час кризи чи катастрофи
A.17.1.2	Реалізація безперервності інформаційної безпеки	Заходи безпеки Організація повинна розробити, задокументувати, реалізувати та підтримувати процеси, процедури та заходи безпеки для гарантування необхідного рівня безперервності щодо інформаційної безпеки під час надзвичайної ситуації

A.17.1.3	Верифікація, перегляд та оцінювання безперервності інформаційної безпеки	Заходи безпеки Організація повинна підтверджувати розроблені та впроваджені заходи безперервності інформаційної безпеки через регулярні інтервали часу для гарантування, що вони дійсні та ефективні протягом надзвичайних ситуацій
A.17.2 Резервне обладнання		
Ціль: Гарантувати доступність обладнання для оброблення інформації.		
A.17.2.1	Доступність обладнання для оброблення інформації	Заходи безпеки Обладнання оброблення інформації має бути впроваджено з резервуванням, достатнім для того, щоб відповідати вимогам доступності
A.18 Відповідність		
A.18.1 Відповідність правовим та контрактним вимогам		
Ціль: Уникнути порушень будь-якого закону, вимог, що діють на підставі закону, нормативних або контрактних зобов'язань, пов'язаних з інформаційною безпекою та будь-якими вимогами щодо безпеки.		
A.18.1.1	Ідентифікація застосовного законодавства та контрактних вимог	Заходи безпеки Усі важливі вимоги, що діють на підставі закону, нормативні чи контрактні вимоги та підхід організації до задоволення цих вимог має бути чітко визначено, задокументовано та актуалізовано для кожної інформаційної системи та організації
A.18.1.2	Права інтелектуальної власності	Заходи безпеки Має бути впроваджено належні процедури забезпечення відповідності законодавчим, нормативним і контрактним вимогам щодо прав інтелектуальної власності та щодо використання запатентованих продуктів програмного забезпечення
A.18.1.3	Захист організаційних записів	Заходи безпеки Відповідно до законодавчих, регуляторних, контрактних і бізнес-вимог важливі записи має бути захищено від втрати, знищення, фальсифікації, несанкціонованого доступу та несанкціонованого використання
A.18.1.4	Захист даних та конфіденційність персональних даних	Заходи безпеки Конфіденційність і захист даних, що ідентифікують особу, має бути забезпечено згідно з вимогами відповідного законодавства та регуляторними вимогами, за наявності.
A.18.1.5	Нормативи щодо криптографічних засобів	Заходи безпеки Криптографічні засоби потрібно використовувати відповідно до всіх застосовних угод, законів та регуляторних вимог
A.18.2 Перевірки інформаційної безпеки		
Ціль: Гарантувати, що інформаційна безпека впроваджена та працює відповідно до організаційних політик та процедур.		
A.18.2.1	Незалежні перевірки інформаційної безпеки	Заходи безпеки Підходи організації до управління інформаційною безпекою та її впровадження (тобто цілі заходів безпеки, заходи безпеки, політики, процеси й процедури для інформаційної безпеки) мають незалежно перевірятися через заплановані інтервали або коли відбуваються значні зміни

A.18.2.2	Відповідність політикам і стандартам безпеки	Заходи безпеки Керівники повинні регулярно перевіряти відповідність оброблення інформації та процедур у межах сфери їх відповідальності належним політикам, стандартам та іншим вимогам щодо безпеки
A.18.2.3	Перевірка технічної відповідності	Заходи безпеки Інформаційні системи потрібно регулярно перевіряти на відповідність політикам і стандартам інформаційної безпеки організації

БІБЛІОГРАФІЯ

1 ISO/IEC 27002:2013 Information technology — Security Techniques — Code of practice for information security controls

2 ISO/IEC 27003 Information technology — Security techniques — Information security management system implementation guidance

3 ISO/IEC 27004 Information technology — Security techniques — Information security management — Measurement

4 ISO/IEC 27005 Information technology — Security techniques — Information security risk management

5 ISO 31000:2009 Risk management — Principles and guidelines

6 ISO/IEC Directives, Part 1, Consolidated ISO Supplement — Procedures specific to ISO, 2012.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

1 ISO/IEC 27002:2013 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки

2 ISO/IEC 27003 Інформаційні технології. Методи захисту. Настанова щодо впровадження системи управління інформаційною безпекою

3 ISO/IEC 27004 Інформаційні технології. Методи захисту. Управління інформаційною безпекою. Вимірювання

4 ISO/IEC 27005 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки

5 ISO/IEC 31000:2009 Управління ризиками. Принципи та настанови

6 ISO/IEC Директиви. Частина 1. Консолідоване ISO доповнення. Процедури, специфічні для ISO, 2012.

ДОДАТОК НА
(довідковий)

ПЕРЕЛІК НАЦІОНАЛЬНИХ СТАНДАРТІВ УКРАЇНИ, ІДЕНТИЧНИХ З МІЖНАРОДНИМИ СТАНДАРТАМИ, ПОСИЛАННЯ НА ЯКІ Є В ЦЬОМУ СТАНДАРТІ

ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)

ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014; IDT)

ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).

Код УКНД 35.040

Ключові слова: інформаційні технології, інформаційна безпека, система управління інформаційною безпекою, методи захисту, заходи безпеки, ресурси СУІБ, відповідальність, інцидент інформаційної безпеки, правила доступу, ризики інформаційної безпеки, оцінка ризиків, впровадження СУІБ, вдосконалення СУІБ, коригувальні дії, аудит.

Редактор **І. Дьячкова**
Верстальник **Л. Мялківська**

Підписано до друку 30.09.2016. Формат 60 × 84 1/8.
Ум. друк. арк. 3,25. Зам. 2107. Ціна договірна.

Виконавець
Державне підприємство «Український науково-дослідний
і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»)
вул. Святошинська, 2, м. Київ, 03115

Свідоцтво про внесення видавця видавничої продукції до Державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції від 14.01.2006 серія ДК № 1647