



НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

---

Інформаційні технології

# НАСТАНОВИ З КЕРУВАННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Частина 4. Вибір засобів захисту  
(ISO/IEC TR 13335-4:2000, IDT)

ДСТУ ISO/IEC TR 13335-4:2005

*Видання офіційне*



БЗ № 11 – 2004/569

Київ  
ДЕРЖСПОЖИВСТАНДАРТ УКРАЇНИ  
2007

## ПЕРЕДМОВА

1 ВНЕСЕНО: Технічний комітет стандартизації України «Інформаційні технології» (ТК-20)

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **А. Анісімов**, д-р фіз.-мат. наук (керівник розроблення); **Д. Літвінов**; **В. Ткаченко**; **О. Фаль**, канд. фіз.-мат. наук

2 НАДАНО ЧИННОСТІ: наказ Держспоживстандарту України від 3 березня 2005 р. № 57 з 2006–07–01

3 Національний стандарт відповідає ISO/IEC TR 13335-4:2000 Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards (Інформаційні технології. Наставни з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту)

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської мови (en)

4 УВЕДЕНО ВПЕРШЕ

---

Право власності на цей документ належить державі.  
Відтворювати, тиражувати і розповсюджувати його повністю чи частково  
на будь-яких носіях інформації без офіційного дозволу заборонено.  
Стосовно врегулювання прав власності треба звертатися до Держспоживстандарту України

Держспоживстандарт України, 2007

## ЗМІСТ

	С.
Національний вступ .....	VII
Передмова до ISO/IEC TR 13335-4 .....	VIII
Вступ до ISO/IEC TR 13335-4 .....	VIII
1 Сфера застосування .....	1
2 Нормативні посилання .....	1
3 Терміни та визначення понять .....	2
4 Мета .....	2
5 Огляд .....	2
6 Вступ до вибору засобів захисту та концепція базової безпеки .....	3
7 Базове оцінювання .....	7
7.1 Визначання типу інформаційної системи .....	8
7.2 Визначання фізичних умов та умов навколишнього середовища .....	8
7.3 Оцінювання наявних/планованих засобів захисту .....	8
8 Засоби захисту .....	9
8.1 Організаційні та фізичні засоби захисту .....	9
8.1.1 Керування інформаційною безпекою та політика безпеки .....	9
8.1.2 Перевіряння узгодженості безпеки .....	10
8.1.3 Реагування на порушення .....	10
8.1.4 Персонал .....	10
8.1.5 Питання експлуатації .....	11
8.1.6 Планування неперервності бізнесу .....	12
8.1.7 Фізична безпека .....	13
8.2 Специфічні засоби захисту інформаційної системи .....	17
8.2.1 Ідентифікація та автентифікація (I&A) .....	17
8.2.2 Контролювання логічного доступу та аудит .....	18
8.2.3 Захист від зловмисного коду .....	19
8.2.4 Керування мережею .....	20
8.2.5 Криптографія .....	20
9 Базовий підхід: вибір засобів захисту відповідно до типу системи .....	24
9.1 Засоби захисту загального застосування .....	24
9.2 Специфічні засоби захисту інформаційної системи .....	25

10 Вибір засобів захисту відповідно до проблем та загроз безпеці .....	26
10.1 Оцінювання проблем безпеки .....	26
10.1.1 Утрата конфіденційності .....	27
10.1.2 Утрата цілісності .....	27
10.1.3 Утрата доступності .....	27
10.1.4 Утрата спостережності .....	28
10.1.5 Утрата автентичності .....	28
10.1.6 Утрата надійності .....	28
10.2 Засоби конфіденційності .....	29
10.2.1 Підслуховування .....	29
10.2.2 Електромагнітне випромінення .....	29
10.2.3 Зловмисний код .....	29
10.2.4 Приховування ідентичності користувача .....	29
10.2.5 Неправильне направлення/перенаправлення повідомлень .....	30
10.2.6 Збої програмного забезпечення .....	30
10.2.7 Крадіжки .....	30
10.2.8 Несанкціонований доступ до комп'ютерів, даних, служб та програм .....	30
10.2.9 Несанкціонований доступ до носіїв даних .....	31
10.3 Засоби контролю цілісності .....	31
10.3.1 Псування носіїв даних .....	31
10.3.2 Помилки обслуговування .....	31
10.3.3 Зловмисний код .....	32
10.3.4 Приховування ідентичності користувача .....	32
10.3.5 Неправильне направлення/перенаправлення повідомлень .....	32
10.3.6 Неспростовність .....	32
10.3.7 Збої програмного забезпечення .....	33
10.3.8 Збої постачання (живлення, кондиціонування повітря) .....	33
10.3.9 Технічні пошкодження .....	33
10.3.10 Помилки передавання .....	33
10.3.11 Несанкціонований доступ до комп'ютерів, даних, служб та програм .....	34
10.3.12 Використання несанкціонованих програм та даних .....	34
10.3.13 Несанкціонований доступ до носіїв даних .....	34
10.3.14 Помилки користувача .....	35

10.4 Засоби захисту доступності .....	35
10.4.1 Руйнівний напад .....	35
10.4.2 Псування носіїв даних .....	35
10.4.3 Збої комунікаційного обладнання та служб .....	36
10.4.4 Вогонь, вода .....	36
10.4.5 Помилки обслуговування .....	36
10.4.6 Зловмисний код .....	36
10.4.7 Приховування особистості користувача .....	36
10.4.8 Неправильне направлення/перенаправлення повідомлень .....	37
10.4.9 Зловживання ресурсами .....	37
10.4.10 Стихійні лиха .....	37
10.4.11 Збої програмного забезпечення .....	37
10.4.12 Збої постачання (живлення, кондиціонування повітря) .....	38
10.4.13 Технічні пошкодження .....	38
10.4.14 Крадіжки .....	38
10.4.15 Перевантаження каналів .....	38
10.4.16 Помилки передавання .....	38
10.4.17 Несанкціонований доступ до комп'ютерів, даних, служб та програм .....	39
10.4.18 Використання несанкціонованих програм та даних .....	39
10.4.19 Несанкціонований доступ до носіїв даних .....	39
10.4.20 Помилки користувача .....	40
10.5 Засоби захисту спостережності, автентичності та надійності .....	40
10.5.1 Спостережність .....	40
10.5.2 Автентичність .....	40
10.5.3 Надійність .....	40
11 Вибір засобів захисту відповідно до детальних оцінок .....	41
11.1 Взаємозв'язок ISO/IEC TR 13335-3 та ISO/IEC TR 13335-4 .....	41
11.2 Принципи вибору .....	41
12 Розроблення базової безпеки організації .....	42
13 Висновки .....	43
Бібліографія .....	44
Додаток А Практичні правила керування інформаційною безпекою .....	44
Додаток В Стандарт базової безпеки ETSI. Функції та механізми .....	46

Додаток С Довідник з базового захисту ІТ .....	47
Додаток D Посібник з комп'ютерної безпеки NIST .....	49
Додаток Е Медична інформатика: категоризація безпеки та захист інформаційних систем для охорони здоров'я .....	50
Додаток F Банківська справа та пов'язані з нею фінансові послуги ТК 68 (ТС 68). Настанова з інформаційної безпеки .....	51
Додаток G Захист контрольованої інформації, на яку не поширюється Закон України «Про державну таємницю». Рекомендації для комп'ютерних робочих станцій .....	53
Додаток H Канадський посібник з безпеки інформаційних технологій .....	54

## НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є тотожний переклад технічного звіту ISO/IEC TR 13335-4:2000 «Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards» (Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту).

Метою цього стандарту є надання настанов, а не конкретних рішень щодо керування інформаційною безпекою. Ті особи в організації, що відповідають за інформаційну безпеку, повинні бути спроможними адаптувати матеріал цього стандарту так, щоб задовольнити свої особливі потреби.

Відповідальний за ISO/IEC TR 13335-4:2000 — технічний комітет ISO/IEC JTC 1.

В Україні відповідальний за цей стандарт — Технічний комітет «Інформаційні технології» (ТК-20).

Багаточастинний міжнародний стандарт ISO/IEC TR 13335 містить п'ять частин.

Частина 1 описує загальні фундаментальні концепції і моделі, використовувані для описування процесів керування безпекою ІТ. Цей документ призначений для адміністраторів, відповідальних за безпеку ІТ та за загальну безпеку в організації.

Частина 2 описує аспекти керування і планування. Її призначено для адміністраторів, до компетенції яких належить взаємодія із системами ІТ організації. До них належать адміністратори ІТ, відповідальні за спостереження над процесами розроблення, реалізації, тестування, постачання або оперування системами ІТ, та адміністратори, відповідальні за отримання максимальної користі від використання систем ІТ.

Частина 3 описує методи захисту, призначена для використання тими, хто задіяний у керуванні протягом усього життєвого циклу проекту, зокрема у процесі планування, проектування, тестування, аналізування або застосування.

Частина 4 містить настанови з вибору засобів захисту, а також як цьому можуть сприяти базові моделі та засоби нагляду. Вона також описує, як ці засоби доповнюють методи захисту, описані в частині 3, і як додаткові методи оцінювання можна використовувати для вибору засобів захисту.

Частина 5 описує настанови щодо організації взаємозв'язку систем ІТ із зовнішніми мережами. Вона містить також настанови щодо вибору і використання засобів захисту для забезпечення безпеки з'єднань і послуг, що надаються цими з'єднаннями і додаткових засобів захисту, застосовування для підключених систем ІТ.

Структура багаточастинного національного стандарту ДСТУ ISO/IEC TR 13335 відповідає структурі міжнародного стандарту ISO/IEC TR 13335 і також містить п'ять частин:

ДСТУ ISO/IEC TR 13335-1:2003 «Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції й моделі безпеки ІТ»;

ДСТУ ISO/IEC TR 13335-2:2003 «Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки ІТ»;

ДСТУ ISO/IEC TR 13335-3:2003 «Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом ІТ»;

ДСТУ ISO/IEC TR 13335-4:200\_ «Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту»;

ДСТУ ISO/IEC TR 13335-5:200\_ «Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанови з керування мережною безпекою».

Ця частина стандарту повністю відповідає міжнародному технічному звіту ISO/IEC TR 13335-4. Ступінь відповідності — IDT.

До стандарту внесено такі редакційні зміни:

— слова «ця частина ISO/IEC TR 13335», «цей звіт» замінено на «цей стандарт».

— у розділі «Нормативні посилання» наведено «Національне пояснення», виділене в тексті рамкою, де надано переклад назв стандартів українською мовою;

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

В Україні чинні стандарти, гармонізовані методом ідентичного перекладу технічних звітів, посилання на які є в ISO/IEC TR 13335-4, а саме:

ДСТУ ISO/IEC TR 13335-1:2003 «Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції й моделі безпеки ІТ»;

ДСТУ ISO/IEC TR 13335-2:2003 «Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки ІТ»;

ДСТУ ISO/IEC TR 13335-3:2003 «Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом ІТ»;

Крім того, в Україні немає чинних національних стандартів, посилання на які є в ISO/IEC TR 13335-4, а саме:

ISO/IEC 10181-2:1996 «Інформаційні технології. Взаємозв'язок відкритих систем. Структура безпеки відкритих систем. Структура автентифікації»;

ISO/IEC 11770-1:1996 «Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Структура».

Копії міжнародних стандартів можна отримати в Головному фонді нормативних документів ДП «УкрНДНЦ».

## ПЕРЕДМОВА ДО ISO/IEC TR 13335-4

ISO (International Organization for Standardization — Міжнародна Організація з Стандартизації) та IEC (International Electrotechnical Commission — Міжнародна Електротехнічна Комісія) формують спеціалізовану систему всесвітньої стандартизації. Національні органи стандартизації країн, що є членами ISO або IEC приймають участь у розробленні міжнародних стандартів через технічні комітети, засновані відповідною організацією для роботи у певних сферах технічної діяльності. Технічні комітети ISO та IEC співпрацюють у сферах взаємного інтересу. Інші міжнародні організації, урядові та неурядові, що співпрацюють з ISO та IEC, також беруть участь у роботі.

Міжнародні стандарти розробляють відповідно до правил, наведених у директивах ISO/IEC, в частині 3.

У галузі інформаційних технологій ISO та IEC заснували спільний технічний комітет — ISO/IEC JTC 1 (Joint Technical Committee 1). Проекти міжнародних стандартів, ухвалені спільним технічним комітетом, направляють до національних органів стандартизації для голосування. Опублікування стандарту як міжнародного потребує затвердження принаймні 75 % національних органів стандартизації, що беруть участь у голосуванні.

За виняткових обставин, коли технічний комітет зібрав дані іншого роду ніж ті, що зазвичай публікують як міжнародний стандарт (наприклад, сучасний стан справ), він може простою більшістю голосів членів, що беруть участь у голосуванні, вирішити опублікувати ці дані як технічний звіт. Технічний звіт за своєю природою є інформаційним і не потребує переглядання, доки дані, що він містить, не перестануть вважатися актуальними або корисними.

Звертається увага на можливість того, що деякі елементи цієї частини ISO/IEC TR 13335 можуть бути предметом патентних прав. ISO та IEC не відповідають за розпізнавання деяких чи всіх таких патентних прав.

Технічний звіт ISO/IEC TR 13335-4 був підготовлений спільним технічним комітетом ISO/IEC JTC 1, *Інформаційні технології*, підкомітетом SC 27, *Методи захисту ІТ*.

Технічний звіт ISO/IEC TR 13335 містить нижченаведені частини під загальною назвою *Інформаційні технології — Настанови з керування безпекою інформаційних технологій*:

Частина 1: Поняття та моделі забезпечення інформаційної безпеки.

Частина 2: Планування та керування інформаційною безпекою.

Частина 3: Методи керування інформаційною безпекою.

Частина 4: Вибір засобів захисту.

Частина 5: Настанови з керування мережною безпекою

## ВСТУП ДО ISO/IEC TR 13335-4

Метою цього технічного звіту (ISO/IEC TR 13335) є надання настанов, а не готових рішень з аспектів керування інформаційною безпекою. Особи, відповідальні за інформаційну безпеку в організації, повинні бути спроможними адаптувати матеріал цього звіту, щоб задовольнити свої потреби.

Основними цілями цього технічного звіту є:

— визначити і описати поняття, пов'язані з керуванням інформаційною безпекою,

— визначити відносини між керуванням інформаційною безпекою та керуванням ІТ взагалі,



— представити декілька моделей, які можна використовувати для пояснення інформаційної безпеки, та

— надати загальну настанову з керування інформаційною безпекою.

Багаточастинний стандарт ISO/IEC TR 13335 містить п'ять частин. Частина 1 описує базові поняття та моделі, що використовуються для описування інформаційної безпеки. Цей матеріал призначений для керівників, відповідальних за інформаційну безпеку, та відповідальних за загальну програму безпеки організації.

Частина 2 описує аспекти керування та планування. Вона доцільна для керівників, до компетенції яких належать інформаційні системи організації. До таких керівників можуть належати:

— керівники IT, обов'язок яких — слідкувати за проектуванням, реалізацією, тестуванням, закупівлею чи експлуатацією інформаційних систем, або

— керівники, відповідальні за сфери діяльності, де використовують інформаційні системи.

Частина 3 описує методи захисту для процесів керування протягом життєвого циклу проекту, таких як планування, проектування, реалізація, тестування, придбання чи експлуатація.

Частина 4 описує настанови з вибору засобів захисту, а також, як цьому можуть сприяти базові моделі та засоби нагляду. Вона також описує, як ці засоби доповнюють методи захисту, описані в частині 3, і як додаткові методи оцінювання можна використовувати для вибору засобів захисту.

**НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ**

---

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

**НАСТАНОВИ З КЕРУВАННЯ БЕЗПЕКОЮ  
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Частина 4: Вибір засобів захисту**

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

**РЕКОМЕНДАЦИИ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**Часть 4: Выбор средств защиты**

INFORMATION TECHNOLOGY

**GUIDELINES FOR THE MANAGEMENT  
OF IT SECURITY**

**Part 4: Selection of safeguards**

---

Чинний від 2006-07-01

**1 СФЕРА ЗАСТОСУВАННЯ**

Цей стандарт надає настанову з вибору засобів захисту, беручи до уваги ділові потреби та проблеми безпеки. Вона описує процес вибору засобів захисту згідно з ризиками безпеки та специфікою навколишнього середовища. Цей стандарт показує, як досягнути достатньо високого рівня захисту, як його підтримувати, застосовуючи базову безпеку. Надається пояснення того, як підхід, описаний у цій частині ISO/IEC TR 13335, забезпечує методи керування інформаційною безпекою, викладені в ISO/IEC TR 13335-3.

**2 НОРМАТИВНІ ПОСИЛАННЯ**

У цьому стандарті є посилання на такі стандарти:

- ISO/IEC TR 13335-1:1997 Information technology — Guidelines for the management of IT Security — Part 1: Concepts and Models
- ISO/IEC TR 13335-2:1997 Information technology — Guidelines for the management of IT Security — Part 2: Managing and Planning IT Security
- ISO/IEC TR 13335-3:1997 Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the Management of Security
- ISO/IEC 10181-2:1996 Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework
- ISO/IEC 11770-1:1996 Information technology — Security techniques — Key Management — Part 1: Framework

#### НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO/IEC TR 13335-1:1997 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Поняття та моделі забезпечення інформаційної безпеки

ISO/IEC TR 13335-2:1997 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Планування та керування інформаційною безпекою

ISO/IEC TR 13335-3:1997 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування інформаційною безпекою

ISO/IEC 10181-2:1996 Інформаційні технології. Взаємозв'язок відкритих систем. Структура безпеки відкритих систем. Структура автентифікації

ISO/IEC 11770-1:1996 Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Структура

### 3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цій частині стандарту використовують такі терміни, визначені в ISO/IEC TR 13335-1: **ідентифікованість** (*accountability*), **цінність** (*asset*), **автентичність** (*authenticity*), **доступність** (*availability*), **базові засоби контролю** (*baseline controls*), **конфіденційність** (*confidentiality*), **цілісність даних** (*data integrity*), **вплив** (*impact*), **цілісність** (*integrity*), **інформаційна безпека** (*IT security*), **політика інформаційної безпеки** (*IT security policy*), **надійність** (*reliability*), **залишковий ризик** (*residual risk*), **ризик** (*risk*), **аналіз ризиків** (*risk analysis*), **керування ризиками** (*risk management*), **засіб захисту** (*safeguard*), **цілісність системи** (*system integrity*), **загроза** (*threat*) та **вразливість** (*vulnerability*). Окрім зазначеного вище використовують такі терміни:

#### 3.1 автентифікація (*authentication*)

Забезпечення гарантії заявленої ідентичності об'єкта (ISO/IEC 10181-2)

#### 3.2 ідентифікація (*identification*)

Процес однозначного визначення унікальної ідентичності об'єкта

### 4 МЕТА

Мета цього стандарту — надати настанову з вибору засобів захисту. Ця настанова застосовна тоді, коли приймають рішення про вибір засобів захисту інформаційної системи:

- відповідно до типу і характеристик інформаційної системи,
- відповідно до загального оцінювання загроз та наявних потреб безпеки,
- відповідно до результатів детального аналізування ризиків.

В доповнення до цієї настанови надані перехресні посилання для того, щоб показати, де вибір засобів захисту може бути підтриманий використанням загально доступних довідників, що містять засоби захисту.

Цей стандарт також визначає, як можна розробити довідник з базової безпеки організації (чи частини організації). Детальні засоби захисту мереж головним чином описані у документах, зазначених у додатках А — Н; на сьогодні ISO розробляє декілька інших документів з мережної безпеки.

### 5 ОГЛЯД

Розділ 6 містить вступ до вибору засобів захисту та концепцію базової безпеки. У розділах 7—10 описано створення базової безпеки для оцінювання інформаційної системи. Для вибору відповідних засобів захисту необхідно зробити деякі основні оцінювання, незалежно від того, чи будуть пізніше виконуватись детальніші дослідження ризику. Ці оцінювання описані в розділі 7, який містить аналіз такого:

- який тип інформаційної системи задіяний (наприклад, окремий ПК або підключений до мережі),
- яке місцезнаходження інформаційної системи та умови навколишнього середовища,
- які засоби захисту вже задіяні та (або) заплановані, і
- чи дають одержані результати оцінювання достатньо інформації для вибору базових засобів захисту для інформаційної системи?

Розділ 8 містить огляд засобів захисту, які мають вибирати, вони поділені на організаційні,

фізичні засоби (їх вибирають відповідно до потреб, наявних проблем і обмежень безпеки) та специфічні засоби інформаційної системи, які, в свою чергу, згруповані категоріями засобів захисту. Для кожної категорії засобів захисту описано найтипівіші представники, охоплюючи коротке пояснення захисту, який вони забезпечуватимуть. Специфічні засоби захисту за цими категоріями та їхній детальний опис можна знайти в документах з базової безпеки, посилання на які наведено в додатках А—Н цього стандарту. Для того, щоб полегшити використання цих документів, у таблиці для кожної категорії заходів наведено перехресні посилання між частинами цього документа та структурними елементами інших документів, зазначених у додатках.

Якщо вирішено, що тип оцінювання, описаний у розділі 7, є достатньо детальним для вибору засобів захисту, то у розділі 9 наведено список придатних засобів для кожної з типових інформаційних систем, описаних у підрозділі 7.1. Якщо засоби захисту вибрані відповідно до типу інформаційної системи, можуть знадобитися окремі базові засоби захисту для автономних робочих станцій, мережних робочих станцій або серверів. Для досягнення потрібного рівня безпеки все, що необхідно для вибору заходів, прийнятих за певних обставин, — це порівняти їх із засобами захисту, що вже є (або заплановані) та реалізувати ті, які ще не реалізовані.

Якщо для вибору ефективних та прийнятних засобів захисту необхідне глибше оцінювання, у розділі 10 описано вибір засобів захисту, який враховує високий рівень безпеки (відповідно до важливості інформації) та можливі загрози. Тому в цьому розділі заходи безпеки наводять відповідно до визначених питань безпеки, враховуючи важливі загрози, і, на закінчення, розглядається приклад. На рисунку 1 наведено шляхи вибору заходів захисту, описаних у розділах 7, 9 та 10.

Розділи 9 та 10 описують спосіб вибору засобів захисту документів з базової безпеки, що можуть застосовуватись, або для інформаційної системи, або для формування набору засобів захисту, застосованих для інформаційних систем за визначених обставин. Зосереджуючись на типі розглянутої інформаційної системи, підхід, що пропонується в розділі 9, створює можливість того, що деякі ризики не управляються в достатній мірі, та що деякі засоби захисту, які вибираються, не є необхідними чи придатними. Підхід, запропонований в розділі 10, для зосередження на проблемах безпеки та пов'язаних з ними загрозах, імовірно, створить більш оптимізований набір засобів захисту. Розділи 9 та 10 можна використовувати для полегшення вибору засобів захисту без більш детального оцінювання у всіх випадках, що знаходяться в межах базового захисту. Однак, якщо використовується більш детальне оцінювання, наприклад, аналіз ризиків, розділи 9 та 10 можуть також підтримувати вибір засобів захисту.

У розділі 11 описано ситуацію, коли необхідне деталізоване аналізування ризиків, унаслідок високих проблем та потреб безпеки. Настанову з аналізування ризиків наведено в ISO/IEC TR 13335-3. Розділ 11 описує взаємозв'язки між частинами 3 та 4 ISO/IEC TR 13335, а також як можуть бути використані результати методів, описаних в частині 3, для вибору засобів захисту. У розділі також описано інші чинники, що можуть впливати на вибір засобів захисту, а саме будь-які обмеження, що мають розглядатися, будь-які юридичні чи інші вимоги, що мають виконуватись тощо. Підхід, зазначений у розділі 11, відрізняється від підходів, описаних у розділах 9 та 10, тим, що у ньому описано настанову з вибору набору засобів захисту, оптимізовану до окремої ситуації. Цей підхід не є базовим, проте може використовуватись для вибору засобів захисту як доповнення до базових за певних обставин. Як альтернатива, цей підхід можна використовувати без урахування базового захисту.

У розділі 12 описано розробляння базового довідника (каталогу) з базової безпеки для цілої організації чи підрозділів організації. Для заснування базового довідника (каталогу) безпеки, мають бути розглянуті засоби захисту, попередньо визначені для інформаційних систем або груп інформаційних систем, та має бути визначений загальний набір засобів захисту. Залежно від потреб, проблем та обмежень безпеки, можуть бути вибрані різні рівні базової безпеки. Означені переваги та недоліки для полегшення вибору прийнятного рішення для кожної організації.

Підсумовуючи зазначимо, що розділ 13 — це підсумки цієї частини ISO/IEC TR 13335, потім наведено бібліографію, а додатки А—Н — це довідники із засобів безпеки, згаданих у розділі 8.

## 6 ВСТУП ДО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ТА КОНЦЕПЦІЯ БАЗОВОЇ БЕЗПЕКИ

Цей розділ дає короткий огляд вибору засобів захисту, та як і коли концепція базової безпеки може бути при цьому використана. Є два головних підходи до вибору засобів захисту, а саме:

використання базового підходу та проведення детального дослідження ризиків. Є декілька різних шляхів проведення детального дослідження ризиків, один з яких детально описаний в ISO/IEC TR 13335-3 і називається детальний аналіз ризиків. У частині 3 також описано переваги та недоліки різних підходів під час аналізування ризиків, і, отже, до вибору засобів захисту.

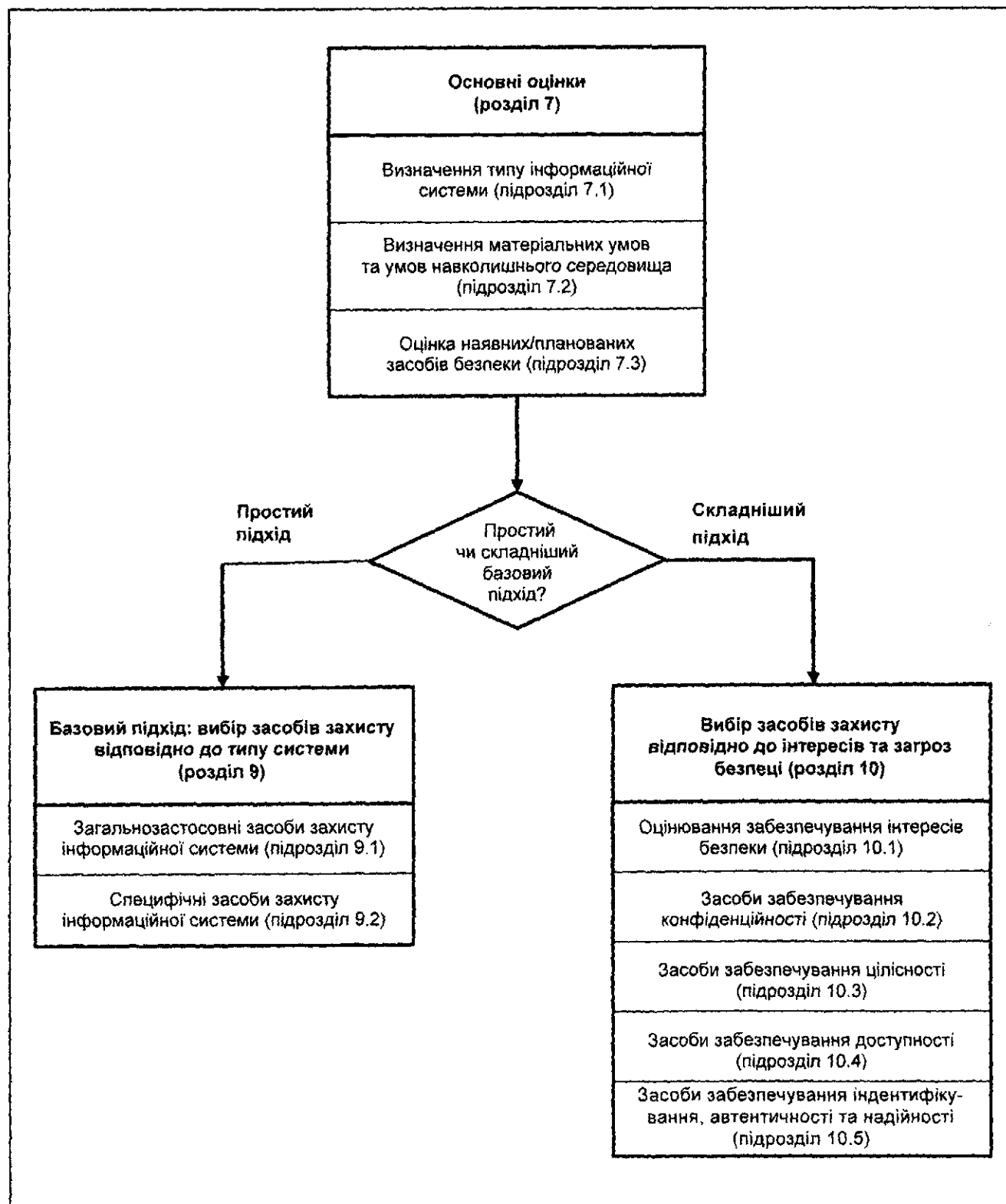


Рисунок 1 — Вибір засобів захисту відповідно до типу системи або відповідно до проблем та загроз безпеці

Проведення детального аналізування ризиків має ту перевагу, що досягається повна картина ризиків. Це необхідно для вибору тих засобів захисту, що зумовлені ризиками, і, відповідно, мають бути реалізовані. Це запобігає забезпеченню занадто великого чи занадто малого захисту. Оскільки цей підхід може вимагати значної кількості часу, зусиль та кваліфікації, він найбільш підходить для інформаційних систем з високим ризиком, тоді як простіший підхід може виявитись достатнім для систем з низьким рівнем ризику. Використання високорівневого аналізування ризиків може визначити системи з низьким рівнем ризику. Цей високорівневий аналіз ризиків не потребує формалізованого чи складного процесу. Засоби захисту для систем з низьким рівнем ризику можуть бути обрані шляхом застосування базової безпеки. Базова безпека забезпечує мінімальний рівень безпеки, визначений організацією для кожного типу ІТ системи. Цей рівень базової безпеки досягається реалізацією мінімального набору засобів захисту, що відомі як базові засоби.

Внаслідок відмінностей в процесі вибору засобів захисту, в цьому документі розглядають два різні шляхи застосування базового підходу:

- використання базового підходу, в якому засоби безпеки рекомендовано вибирати відповідно до типу та характеристик ІТ системи, що розглядається;
- використання базового підходу, в якому засоби безпеки рекомендовано вибирати відповідно до проблем та загроз безпеки, також враховувати і систему, що розглядається.

На рисунку 1 як частині рисунка 2, що відтворює взаємозв'язки між ISO/IEC TR 13335-4 та ISO IEC/TR 13335-5 розглянуто різні паралельні способи вибору засобів захисту, описані у цьому документі.

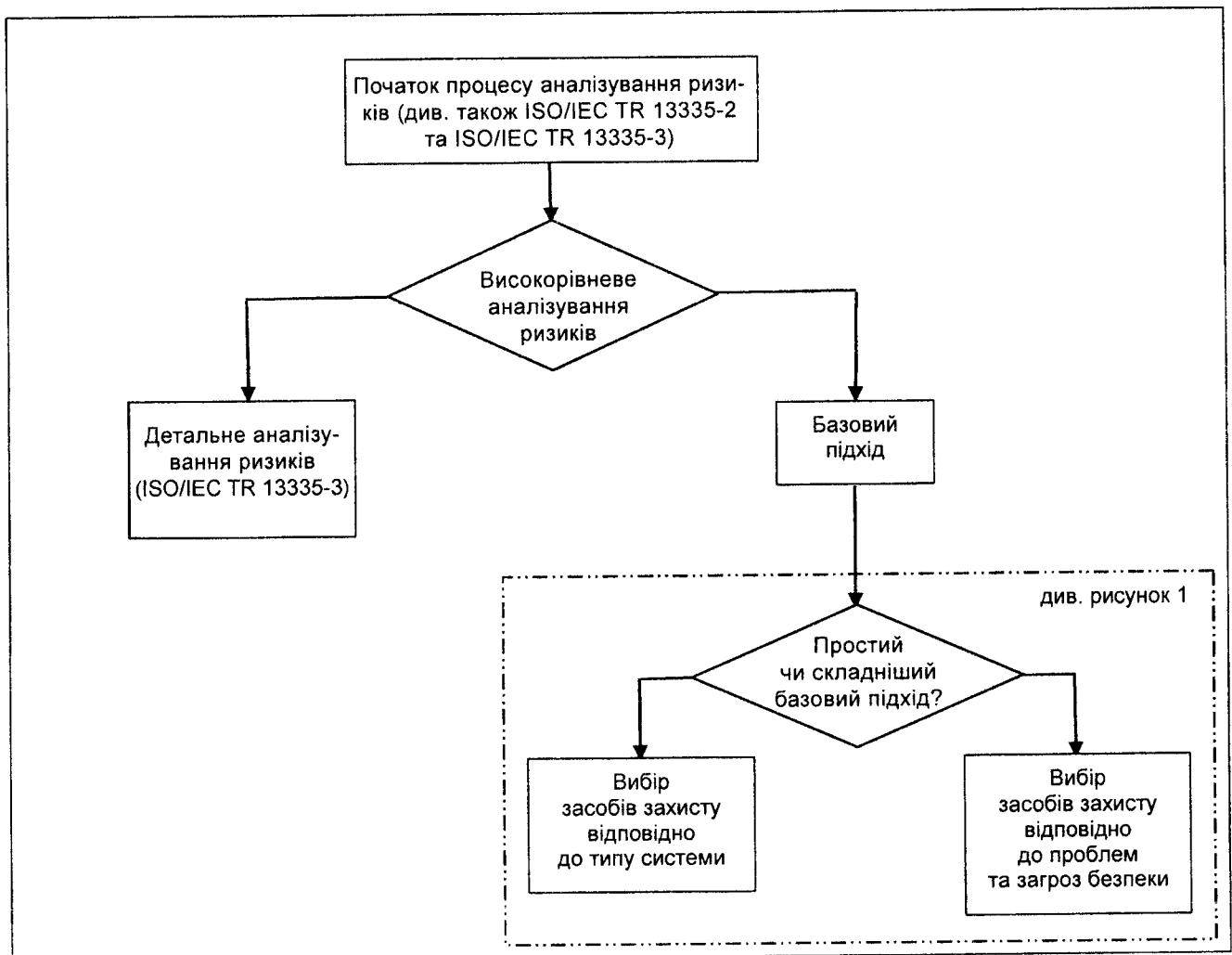


Рисунок 2 — Способи вибору засобів захисту

Базовий підхід, що буде використаний, треба вибирати відповідно до ресурсів, які можуть бути витрачені у процесі вибору усвідомлених проблем безпеки, а також типу і характеристик інформаційної системи, що розглядається. Якщо організація не бажає витрачати багато часу та зусиль на вибір засобів захисту (з будь-якої причини), то можна скористатися базовим підходом, що пропонує засоби захисту без подальшого оцінювання. Однак, якщо ділові процеси організації до певної міри залежать від інформаційної системи чи послуг та (або) оброблювана інформація контролюється, то дуже ймовірно, що будуть необхідні додаткові засоби захисту. В цьому випадку настійно рекомендується, проводити високорівневий огляд важливості інформації та можливих загроз для того, щоб мати краще уявлення про засоби захисту, потрібні для найефективнішого захисту інформаційної системи. Якщо ділові процеси організації сильно залежать від інформаційної системи чи послуг, та (або) оброблена інформація є дуже чутливою, ризики можуть бути високі, і детальне аналізування ризиків є найкращим шляхом визначення прийнятних засобів захисту.

Специфічні засоби захисту повинні призначатися на основі детального аналізування ризиків, якщо

- тип інформаційної системи, що розглядається, не відповідає типам, описаним у цьому стандарті,

- діяльність чи потреби безпеки не відповідають рішенням, запропонованим у цих розділах, або

- детальніше оцінювання є виправданим у разі потенційно високих ризиків, чи важливості інформаційної системи для діяльності організації.

Треба зазначити, що навіть, коли виконано детальне аналізування ризиків, все ще доцільно застосувати до системи базові засоби захисту.

Перше рішення, яке повинна ухвалити організація — чи використовувати базовий підхід сам по собі, чи як частину більш повної стратегії аналізування ризиків (див. ISO/IEC TR 13335-3). У разі прийняття цього рішення треба зазначити, що під час використання базового підходу самого по собі, результатний процес вибору засобів захисту може дати менш оптимізовану безпеку, ніж прийнята ширша стратегія аналізування ризиків. Однак, менші кошти та ресурси, необхідні під час вибору засобів забезпечення безпеки, та досягнення принаймні мінімального рівня безпеки для всіх інформаційних систем можуть бути причинами для прийняття рішення про використання тільки базового підходу.

Базовий захист для інформаційної системи може бути досягнутий через визначення та застосування набору відповідних засобів захисту, що є прийнятним за обставин наявності низького ризику, тобто вони задовольняють, принаймні, мінімальні потреби безпеки. Наприклад, прийнятні засоби захисту можуть бути визначені через каталоги, що містять набори засобів захисту безпеки від більшості загальних загроз для різних типів ІТ. Ці каталоги засобів захисту містять інформацію про категорії засобів захисту чи про окремі засоби, але загалом не зазначають, які засоби захисту треба застосовувати в конкретних обставинах. Можливо, якщо інформаційні системи організації (чи частини організації) є дуже схожі за природою та послугами, які вони надають, засоби захисту, вибрані за базовим підходом, можуть бути застосовані до всіх систем ІТ. На рисунку 3 показано різні способи використання базового підходу, який описано в цій частині ISO/IEC TR 13335.

Якщо організація вирішує впровадити базову безпеку до організації в цілому або її підрозділів, необхідно вирішити, для яких підрозділів організації прийнятні засоби захисту, і який рівень безпеки повинен забезпечувати цей захист. У більшості випадків, коли використовують базову безпеку, не застосовують менший рівень безпеки, доки не будуть реалізовані додаткові засоби захисту, обґрунтовані та необхідні для керування середніми та великими ризиками. Як альтернатива, базова безпека може визначити середній рівень для організації, тобто дозволяються винятки вище і нижче базового рівня, якщо вони були обґрунтовані, наприклад, результатами аналізування ризиків.

Однією з переваг базової безпеки є те, що її застосовують до груп інформаційних систем, і всюди в цій групі можна покладатися на визначений рівень безпеки. В цих умовах зазвичай найкориснішим є розробити і вести базовий каталог засобів захисту в межах організації чи відділу.

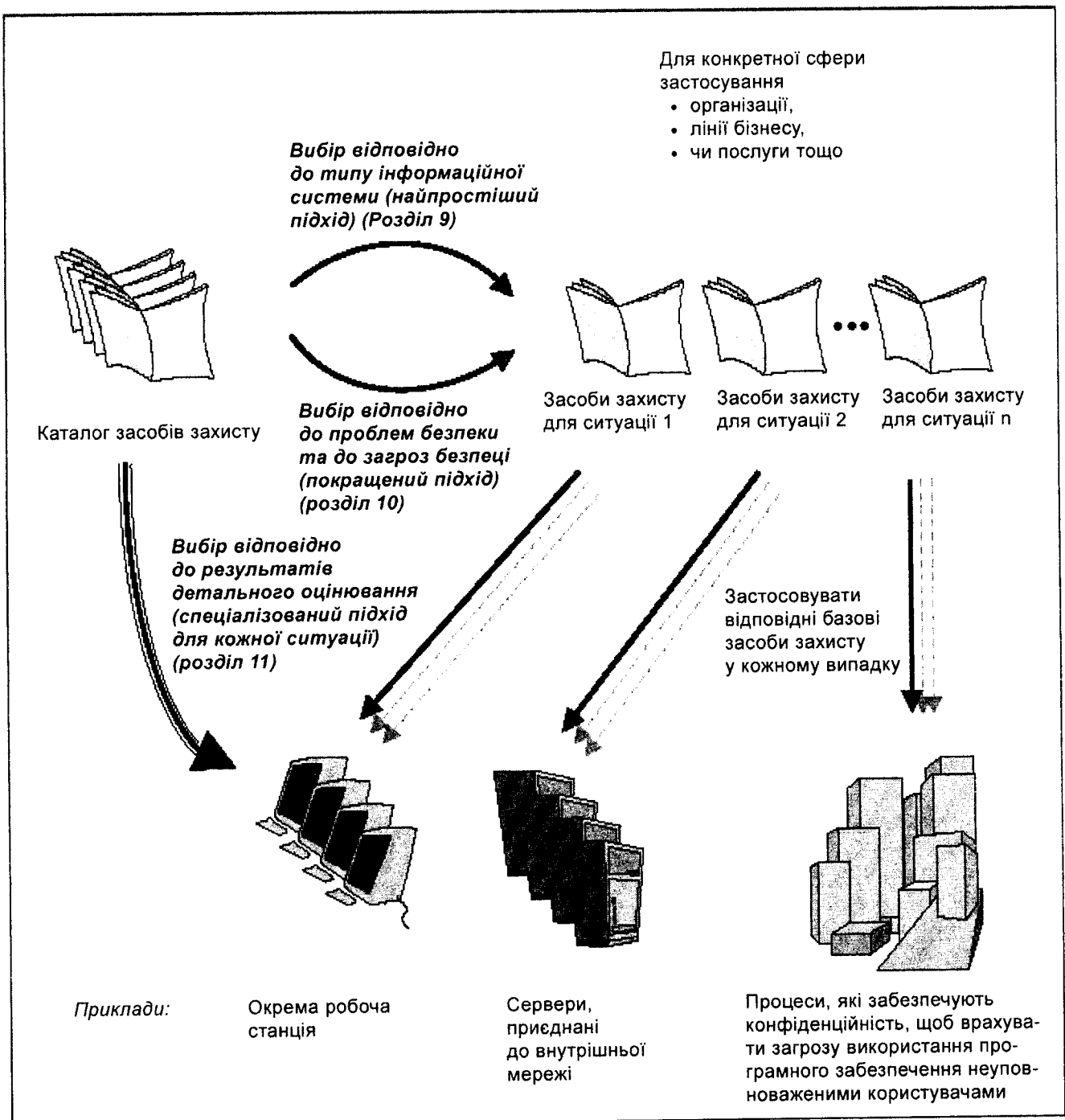


Рисунок 3 — Базове оцінювання під час вибору засобів захисту

## 7 БАЗОВЕ ОЦІНЮВАННЯ

Процес вибору засобів захисту завжди потребує певного знання типу та характеристик інформаційної системи, що розглядається, (наприклад, окрема робоча станція або робоча станція, підключена до мережі), оскільки це має суттєвий вплив на вибрані засоби захисту. Корисно мати план інфраструктури, які містять будівлі, кімнати тощо. Інший важливий чинник, пов'язаний із вибором засобів захисту — це оцінювання наявних та (або) запланованих засобів захисту. Це звільняє від зайвої роботи та марнування часу, зусиль та коштів. Тому настійно рекомендується, щоб оцінювання, описане в розділі 7, завжди використовували як основу для вибору засобів захисту. Коли вибирають засоби захисту, треба брати до уваги вимоги бізнесу та підхід організації



до безпеки (див. ISO/IEC TR 13335-2). Нарешті, необхідно визначити, чи надають ці результати оцінювання достатньо інформації для вибору базових засобів захисту, чи необхідне детальніше оцінювання (див. розділ 10) або детальне аналізування ризиків (див. розділ 11).

### 7.1 Визначання типу інформаційної системи

Для оцінювання наявної чи запланованої інформаційної системи її треба порівняти з нижченаведеними компонентами та визначити складники, визначальні для системи. Засоби захисту, що пропонуються для кожного з перерахованих нижче компонентів, наведено в розділі 9. Компоненти для вибору такі:

- окрема робоча станція,
- робоча станція (клієнт без спільних ресурсів), підключена до мережі,
- сервер чи робоча станція зі спільними ресурсами, підключена до мережі.

### 7.2 Визначання фізичних умов та умов навколишнього середовища

Оцінювання оточення охоплює визначання фізичної інфраструктури, що підтримує наявну чи заплановану інформаційну систему, так само як і пов'язані з нею наявні та (або) заплановані засоби захисту. Оскільки всі засоби захисту мають бути сумісними з навколишнім середовищем, ці оцінки є істотними для успішного вибору. Нижченаведені питання можуть надати допомогу під час досліджування інфраструктури. Читач повинен також врахувати вплив навколишнього середовища та будь-які інші обставини.

Розташування та будівля:

- де розташована будівля — на своїй власній ділянці з огорожею по периметру, чи на вулиці в місці з інтенсивним рухом транспорту тощо?
- будівля зайнята однією організацією чи зайнята багатьма організаціями?
- якщо будівля зайнята багатьма організаціями, то хто ці мешканці?
- де знаходяться зони безпеки?

Керування доступом:

- хто має доступ до будівлі?
- чи є система керування фізичним доступом?
- наскільки міцна конструкція будівлі?
- наскільки міцні двері, вікна тощо та як вони захищені?
- чи охороняється будівля, якщо так, то цілодобово чи тільки протягом робочого часу?
- чи є в будівлі та (або) кімнаті, в якій розташоване критичне інформаційне обладнання, сигналізація для захисту від вторгнень?

Захист на місці:

- як захищається кімната (кімнати), що містить інформаційну систему?
- яка система виявлення пожежі, сигналізація та система гасіння встановлені, та де вони знаходяться?
- яка система виявлення витоку води/рідини, можливості її виведення та сигналізації?
- чи є допоміжні засоби, такі як система безперебійного живлення, водопровід та кондиціювання повітря (для контролю температури та вологості)?

Відповідаючи на ці питання, можна легше виявити наявні фізичні та пов'язані з ними засоби захисту. Варто відмітити, що під час дослідження місцезнаходження будівлі, необхідно одночасно з'ясувати все, що стосується дверей, замків та контролю і порядку фізичного доступу, ця процедура не займає багато часу.

### 7.3 Оцінювання наявних/планованих засобів захисту

Після оцінювання умов навколишнього середовища та компонентів інформаційної системи треба визначити всі інші засоби захисту: вже наявні та заплановані. Це необхідно, щоб уникнути повторного вибору наявних чи запланованих засобів, а знання цих засобів захисту допомагає вибрати інші засоби, що будуть діяти разом з ними. Коли вибирають засоби захисту, треба розглядати сумісність наявних засобів захисту з вибраними. Засіб захисту може бути несумісний з іншими засобами захисту чи унеможливлюватиме успішну діяльність та захист, що забезпечується.

Для визначення наявних чи планованих засобів захисту, можуть бути корисними такі дії:

- перегляньте документи, що містять інформацію про засоби захисту (наприклад, плани чи концепції інформаційної безпеки) — якщо процес убезпечення добре документований, всі наявні чи заплановані засоби та статус їх реалізації повинні бути там перераховані,

— перевірте з відповідальними особами (наприклад, керівник інформаційної безпеки, управитель будинком чи директор-розпорядник) та користувачами, які засоби захисту дійсно реалізовані для інформаційної системи, що розглядається, та

— продивіться схему розташування засобів захисту в будівлі, порівняйте запроваджені засоби захисту зі списком тих, що мають бути, та перевірте як запроваджено засоби захисту, чи вони працюють коректно та ефективно.

Може бути виявлено, що наявні засоби захисту перевищують поточні потреби. В цьому випадку, треба розглянути можливість видалення цих засобів. Якщо розглядати вилучення надлишкових засобів чи засобів, що не є необхідними, треба взяти до уваги чинники безпеки та вартості. Оскільки засоби захисту впливають один на одного, видалення надлишкових засобів може зменшити загальну безпеку. Треба зазначити, що іноді дешевше залишити ці засоби на місці, ніж вилучати їх, чи, особливо, якщо засоби захисту мають високу вартість обслуговування, дешевше вилучити їх.

## 8 ЗАСОБИ ЗАХИСТУ

У цьому розділі подано огляд засобів захисту, які можна реалізувати для підвищення безпеки. Деякі з цих засобів є механізмами, інші можуть розглядатися, як процедури, яких треба дотримуватись. Організаційні та фізичні засоби, що можуть бути застосовані в інформаційних системах, наведено у підрозділі 8.1. Засоби захисту, специфічні для окремих ІТ систем, розглянуто в 8.2. Треба зазначити, що засоби захисту описані незалежно від способу, яким вони можуть бути вибрані, тобто деякі з цих засобів захисту можуть бути вибрані одним способом, інші можуть бути визначені тільки після проведення детального аналізування ризиків.

Для полегшення опису різних типів засобів захисту, були введені категорії цих засобів. Нижченаведені підрозділи містять короткий опис цих категорій та які типи засобів захисту їм відповідають. У додатках від А до Н наведено посилання на джерела, наведені у бібліографії в кінці цього документа (див. сторінку 35), в яких зазначено, де можна знайти ґрунтовнішу інформацію про засоби захисту, згадані тут.

### 8.1 Організаційні та фізичні засоби захисту

У кінці цього підрозділу наведені таблиці, що стосуються кожного пункту, в яких зазначено, де можна знайти додаткову інформацію про згадані категорії засобів захисту.

#### 8.1.1 Керування інформаційною безпекою та політика безпеки

Ця категорія засобів захисту містить всі ті засоби, що стосуються керування інформаційною безпекою, планування якої повинно містити відповідальність за ці процеси, та іншу діяльність, що стосується безпеки. Ці засоби захисту вже було введено в перших трьох частинах ISO/IEC TR 13335. Мета цих засобів захисту — досягнути прийнятного рівня безпеки в організації. Засоби захисту в цій сфері наведено нижче.

##### 1 Корпоративна політика інформаційної безпеки.

Треба розробити письмовий документ, який має містити правила, вказівки та практичні рекомендації з керування цінностями, їх захист і поширення в організації. Він повинен містити відомості про необхідність документів з інформаційної безпеки та настанову щодо їх змісту.

##### 2 Політика безпеки інформаційної системи.

Для кожної інформаційної системи має бути розроблена політика її безпеки, що описує засоби захисту, які існують чи мають бути реалізовані. Також вона повинна містити процедури, що стосуються захисту цієї системи, також, за потреби, виклад проблем безпеки та (або) ризиків, що обґрунтовують засоби захисту.

##### 3 Керування інформаційною безпекою

Керування інформаційною безпекою має бути формалізованим та скоординованим у межах організації відповідно до її розміру, наприклад, заснуванням комітету інформаційної безпеки та призначенням особи (часто керівник інформаційної безпеки), відповідальної за безпеку кожної інформаційної системи.

##### 4 Розподіл обов'язків

Обов'язки стосовно інформаційної безпеки організації, повинні бути чітко задокументовані та розподілені відповідно до корпоративної політики інформаційної безпеки та політики безпеки інформаційної системи.

### **5 Організація інформаційної безпеки**

Всі ділові процеси, що можуть підтримати інформаційну безпеку (наприклад, закупки, співробітництво з іншими організаціями) повинні бути організовані так, щоб надійно забезпечити цю підтримку.

### **6 Визначення і оцінка цінностей**

Мають бути визначені всі цінності в організації та в ІТ системі і оцінене їх значення для ведення бізнесу.

### **7 Затвердження інформаційних систем**

Затвердження інформаційних систем повинне відбуватися відповідно до політики інформаційної безпеки. Процес затвердження має метою виявити, чи реалізовані засоби безпеки дійсно забезпечують відповідний рівень захисту. Треба брати до уваги, що інформаційна система може охоплювати мережі та основні засоби зв'язку.

#### **8.1.2 Перевіряння узгодженості безпеки**

Важливо, щоб підтримувалась узгодженість зі всіма необхідними засобами захисту, важливими законами, правилами та нормами, оскільки будь-який засіб захисту, правило чи політика можуть працювати до тих пір, поки користувачі їх застосовують, а системи узгоджуються з ними. Засоби захисту в цій сфері наведено нижче.

##### **1 Узгодженість з політикою інформаційної безпеки та засобами захисту**

Треба проводити регулярні перевіряння для гарантування того, що всі засоби захисту, впроваджені на місці, як зазначено в корпоративній політиці безпеки та інших важливих документах, наприклад документах чинних процедур безпеки та надзвичайних планах, реалізовані коректно і використовуються коректно та ефективно (кінцевими користувачами також), і за необхідності, проведено тестування.

##### **2 Узгодженість з правовими та регуляторними вимогами**

Перевіряння узгодженості, згадані вище, повинні підтвердити, що виконуються всі правові та регуляторні вимоги, чинні в країні, чи країнах, де задіяна інформаційна система. Там, де це законодавство чинне, воно охоплює і законодавство відносно захисту та недоторканності даних, копіювання програмного забезпечення, захисту записів, що ведуться в організації, зловмисного використання інформаційних систем чи криптографії.

#### **8.1.3 Реагування на порушення**

Кожен в організації має бути обізнаним з необхідністю звітувати про порушення безпеки, в тому числі і збої програмного забезпечення та виявлену недосконалість так швидко, як це можливо. Організація повинна забезпечити схему звітування, яка зробить це можливим. Реагування на порушення містить:

##### **1 Звітування про порушення безпеки.**

Кожен працівник повинен усвідомлювати, що він зобов'язаний звітувати про порушення безпеки. Інструментальні засоби також можуть визначати порушення та звітувати про них. Для полегшення ефективного реагування на порушення, організація повинна впровадити схему звітування та точки контакту в організації.

##### **2 Звітування про недосконалість безпеки.**

Якщо користувачі помічають будь-яку недосконалість системи, що стосується безпеки, вони повинні повідомити про неї відповідальній особі так швидко, наскільки це можливо.

##### **3 Звітування про збої програмного забезпечення.**

Якщо користувачі помічають будь-які збої програмного забезпечення, що стосуються безпеки, вони повинні звітувати про них відповідальній особі так швидко, наскільки це можливо.

##### **4 Керування інцидентами.**

Має бути процес керування, що забезпечує захист від інцидентів, їх виявлення та звітування, та відповідне реагування на інцидент. Інформація про порушення повинна збиратися і оцінюватись щоб унеможливити інциденти в майбутньому та зменшити збитки від них.

#### **8.1.4 Персонал**

Засоби захисту в цій категорії повинні зменшувати ризики безпеки, що виникають від помилок або зловмисного чи незловмисного порушення правил безпеки персоналом (який працює постійно чи тимчасово). Засоби захисту в цій сфері наведено нижче.

### **1 Засоби захисту для постійного та тимчасового штату.**

Всі працівники мають знати про свої обов'язки стосовно безпеки. Усі процедури стосовно безпеки, яких слід дотримуватись персоналу, мають бути сформульовані у документі. Працівників треба перевіряти перед влаштуванням на роботу, та, за потреби, підписувати договір про нерозголошення інформації.

### **2 Засоби захисту для договірної персоналу**

Договірний персонал (наприклад прибиральники чи обслуговувальний персонал) треба контролювати так само, як інших відвідувачів. Договірний, звичайно довгостроковий, персонал повинен підписувати договір про нерозголошення перед тим, як отримає доступ (фізичний чи логічний) до комп'ютерного обладнання організації.

### **3 Обізнаність у питаннях безпеки та навчання**

Для підтримання поінформованості весь персонал, що використовує, розробляє, підтримує чи має доступ до комп'ютерного обладнання, повинен отримувати регулярні інструкції та інші матеріали. Це має забезпечити персоналу розуміння важливості для бізнесу оброблюваної інформації, пов'язаних з нею загроз, ризиків тощо, і, отже, розуміння того, для чого потрібні засоби захисту. Користувачі також мають бути навчені використовувати комп'ютерне обладнання коректно, щоб унеможливити помилки. Для вибраного персоналу, наприклад, керівників інформаційної безпеки, адміністраторів безпеки, можливо необхідно більш специфічне навчання безпеці.

### **4 Дисциплінарний процес.**

Всі працівники повинні знати про наслідки (зловмисних чи незловмисних) порушень політики безпеки організації в цілому та політик безпеки окремих інформаційних систем, або будь-яких інших задокументованих домовленостей, пов'язаних з безпекою.

### **8.1.5 Питання експлуатації**

Засоби захисту в цій сфері охоплюють процедури підтримування безпечного, правильного та надійного функціонування комп'ютерного обладнання та пов'язаних з ним систем. Більшість цих засобів захисту може бути реалізована шляхом запровадження організаційних процедур. Експлуатаційні засоби захисту треба запроваджувати в поєднанні з іншими, наприклад, фізичними та технічними засобами. Засоби захисту в сфері питань експлуатації наведено нижче.

#### **1 Керування конфігурацією та змінами**

Керування конфігурацією — це процес відстежування змін інформаційних систем. Основна його мета щодо безпеки — переконатися, що ці зміни в ІТ системах не зменшують ефективність засобів захисту та безпеки в цілому. Керування змінами може сприяти визначенню нових включень засобів захисту безпеки, коли трапляються зміни в ІТ системах.

#### **2 Керування навантаженнями**

Керування навантаженнями треба використовувати, щоб уникнути збоїв через неадекватні потужності. Коли оцінюються необхідні навантаження для інформаційної системи, треба брати до уваги майбутні навантаження та поточні тенденції.

#### **3 Документація**

Всі аспекти конфігурацій та діяльності ІТ систем повинні документуватися для забезпечення неперервності та стабільності. Безпеку інформаційної системи також треба документувати в частині політики безпеки інформаційної системи, в документах чинних процедур безпеки, та звітах і планах, що стосуються стратегії забезпечення неперервності бізнесу. Документація має бути актуалізованою та доступною.

#### **4 Обслуговування**

Комп'ютерне обладнання потрібно правильно обслуговувати для забезпечення постійної надійності, доступності та цілісності. Всі вимоги безпеки, що мають задовольнятися постачальниками обслуговування, повинні бути повністю задокументовані в договорах на обслуговування. Обслуговування треба виконувати відповідно до договору з постачальником та тільки уповноваженим персоналом.

#### **5 Відстежування змін, що стосуються безпеки.**

Зміни впливів, загроз, вразливостей та ризиків, а також їхніх характеристик треба відстежувати. Відстежування має охоплювати як нові, так і старі аспекти. Навколишнє середовище, в якому розташована система, також треба відстежувати.

#### **6 Результати аудиту та ведення журналів.**

Можливості аудиту та ведення журналів серверів (наприклад, записування результатів аудиту та засоби аналізування), мереж (наприклад, засоби аудиту брандмауерів та маршрутизаторів)

і програмного забезпечення (наприклад, засоби аудиту програм обміну повідомленнями чи програм оброблення транзакцій) треба використовувати для запису деталей подій, що стосуються безпеки. Вони охоплюють деталі подій, визнаних неповноважними чи помилковими, а також деталі звичайних подій, що мають бути проаналізовані пізніше. Результати аудиту та журнали треба регулярно переглядати для виявлення неповноважних дій, що дозволить приймати відповідні корегувальні заходи. Події, записані в журналах, треба аналізувати також з метою виявлення повторення схожих подій, що можуть вказувати наявність вразливостей чи загроз, засоби захисту від яких є неадекватними. Такий аналіз може також виявити закономірності в непов'язаних, на перший погляд, подіях, що може дозволити ідентифікувати людей, що виконують неповноважні дії, чи кореневу причину проблеми з безпекою.

**Примітка.** В цьому тексті «можливості аудиту» систем та програмного забезпечення, а також «можливості ведення журналів» використовують для позначення одного й того ж. Доки такі можливості можна використовувати для підтримування аудиту фінансової цілісності, вони задовольняють тільки частині вимог для такої діяльності, і читач повинен усвідомлювати використання цієї термінології.

### **7 Тестування безпеки**

Тестування безпеки треба використовувати, щоб все комп'ютерне обладнання та всі пов'язані програмні компоненти працювали безпечно. Тестування безпеки здійснюють, щоб перевірити на відповідність вимогам безпеки, визначеним у політиці безпеки інформаційної системи та планах проведення тестування, а також має бути встановлено критерій прийняття для демонстрування того, що необхідний рівень безпеки досягнуто.

### **8 Контроль носіїв інформації**

Контроль носіїв інформації охоплює низку засобів захисту для забезпечення фізичного захисту та захисту, що стосується навколишнього середовища, і також обліку стрічок, дисків, роздруківок та інших носіїв інформації. Вони містять маркування, ведення журналів, перевіряння цілісності, захист від фізичного доступу, від навколишнього середовища, передавання та безпечне знищення.

### **9 Гарантоване вилучення інформації**

Конфіденційність інформації, попередньо записаної на запам'ятовувальний пристрій, має бути збереженою, якщо ця інформація більше не потрібна. Треба забезпечити, щоб файли, які містять конфіденційні матеріали, були стерті та фізично перезаписані, або ж знищені іншим способом — активація функцій вилучення не завжди це робить. Засоби, схвалені відповідальним персоналом (наприклад, керівником інформаційної безпеки) мають бути доступні всім користувачам для повного та безпечного вилучення даних.

### **10 Розподіл обов'язків**

Для мінімізації ризиків та можливостей зловживання правами треба запроваджувати розподіл обов'язків там, де це потрібно та можливо. Зокрема, обов'язки та функції, що в поєднанні можуть призвести до обминання засобів захисту чи аудиту, або надмірних привілеїв для працівника, потрібно тримати роздільно.

### **11 Правильне використання програмного забезпечення**

Щоб матеріал не копіювався, треба забезпечити захист авторського права, через виконання ліцензійної угоди для використовування комерційного програмного забезпечення.

### **12 Контроль змін програмного забезпечення**

Контроль змін може бути запроваджений для підтримування цілісності програмного забезпечення, коли вносять зміни (контроль змін програмного забезпечення застосовується тільки до програм, оскільки керування конфігурацією та змінами розглянуто в позиції переліку 1 цього пункту, застосовується до інформаційних систем та їх оточення як цілого). Треба встановити процедури контролю змін до програмного забезпечення, що керують всіма змінами та гарантують, що безпека підтримується протягом всього процесу. Вони охоплюють авторизацію змін, розгляд безпеки проміжних рішень та перевіряння безпеки остаточного рішення.

### **8.1.6 Планування неперервності бізнесу**

Для захисту бізнесу, особливо критичних ділових процесів, від наслідків великих збоїв чи катастроф та для мінімізації пошкоджень, спричинених такими подіями, має існувати чинник ефективної неперервності бізнесу, охоплюючи планування непередбачуваних обставин/відновлення після катастроф, стратегію і план(и). Він містить такі засоби захисту.

### **1 Стратегія неперервності бізнесу**

Стратегія неперервності бізнесу, охоплюючи планування непередбачуваних обставин/відновлення після катастроф, повинна бути сформульована та задокументована відповідно до інформаційної системи, що розглядається, на основі визначених потенційних ударів спричинених недоступністю, модифікаціями та знищенням, нанесених недружнім бізнесом.

### **2 План неперервності бізнесу**

На основі стратегії неперервності бізнесу, треба розробити та задокументувати план(и) неперервності бізнесу, охоплюючи плани непередбачуваних обставин та відновлення після катастроф.

### **3 Тестування та оновлення плану неперервності бізнесу**

Перед прийняттям план неперервності бізнесу має бути ретельно відтестований для гарантування того, що він працює в «реальних» обставинах, та доведено до відома всіх відповідних працівників. Оскільки плани неперервності бізнесу можуть швидко старіти, важливо їх регулярно оновляти. Стратегію неперервності бізнесу треба за необхідності оновляти.

### **4 Резервування**

Для всіх важливих файлів та інших ділових даних, важливих системних програм та документації потрібно робити резервні копії. Частоту резервування треба узгоджувати з важливістю інформації та плану неперервності бізнесу. Резервні копії треба зберігати у безпечному та віддаленому місці, а відновлення перевіряти регулярно для надійності.

### **8.1.7 Фізична безпека**

Засоби захисту в цій сфері пов'язані з фізичним захистом. Їх треба розглядати в поєднанні з визначенням навколишнього середовища, описаного в підрозділі 7.2. Положення декількох нижченаведених підрозділів поширюються на будівлі, безпечні зони, комп'ютерні кімнати та офіси. Вибір засобів захисту залежить від того, яка частина будівлі розглядається. Засоби захисту в цій сфері наведено нижче.

#### **1 Матеріальний захист**

Фізичні засоби для захисту будівлі охоплюють паркани, фізичний контроль доступу, міцні стіни, двері та вікна. Зони будівлі, які підлягають захисту, треба захищати від несанкціонованого доступу за допомогою системи контролю фізичного доступу, охорони тощо. Зони захисту можуть бути необхідними для комп'ютерного обладнання, такого, як сервери, з відповідним програмним забезпеченням та даними, що підтримують важливі ділові операції. Доступ до таких зон захисту повинен обмежуватись мінімальною кількістю необхідного персоналу, а подробиці треба записувати в журналі. Все обладнання для діагностування та контролю треба надійно зберігати та ретельно контролювати під час використання.

#### **2 Протипожежний захист**

Обладнання та прилеглі зони, охоплюючи підхід до них, треба захищати від поширення вогню з будь-якого місця в будівлі чи з суміжних будівель. Небезпека загоряння поблизу кімнат/зон, де розміщено обладнання, має бути мінімізована. Також треба забезпечити захист від вогню, що займається та (або) поширюється на всі кімнати/зони, де розташоване ключове обладнання. Засоби захисту мають уникати сигналізацію на виявлення вогню та диму і систему гасіння. Потрібно потурбуватися про те, щоб захист від пожежі не призвів до пошкодження комп'ютерних систем від води чи інших засобів гасіння.

#### **3 Захист від води/рідини**

Цінне обладнання не треба розташовувати на майданчиках, де можливі значні затоплення та витоки води чи іншої рідини. Відповідний захист має бути забезпечений там, де є значна загроза затоплення.

#### **4 Захист від стихійних лих**

Будівлі, де розміщено ключове обладнання треба захищати від ударів блискавки. Також це обладнання безпосередньо треба захищати від цих ударів. Захист від інших стихійних лих можна досягти, уникаючи районів, де вони можуть статися (якщо це можливо), а також запроваджуючи стратегії та планування неперервності бізнесу.

#### **5 Захист від крадіжок**

Для контролю запасів кожна одиниця обладнання має бути ретельно облікована та занесена до опису майна. Охоронцям/реєстраторам треба перевіряти обладнання чи носії інформації на предмет винесення їх з кімнати/зони чи будівлі без авторизації. Секретна інформація та патентоване програмне забезпечення, що зберігається на портативних носіях інформації (наприклад, дискетах), треба захищати відповідно.

### 6 Електричне живлення та кондиціонування повітря

За потреби все комп'ютерне обладнання треба захищати від збоїв живлення. Треба забезпечити придатне електропостачання, а також за потреби впровадити безперебійне живлення. Інша мета захисту — забезпечити необхідну температуру та вологість.

### 7 Прокладання кабелю

Кабелі електричного живлення та зв'язку, які передають дані чи підтримують інформаційні послуги, потребують захисту від перехвату, пошкодження чи перевантаження. Кабелі мають бути фізично захищені від випадкового чи зловмисного пошкодження, вибрані та прокладені відповідно до їх призначення; ретельне планування, що передбачає майбутні розроблення, дозволяє уникнути багатьох проблем. Там, де це об'єднується і можливо, кабелі треба захищати від прослуховування.

**Таблиця 8.1.1** — Керування інформаційною безпекою та політикою безпеки

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Корпоративна політика інформаційної безпеки	3.1	—	1.1, 1.2	5.1	*.3.1.1	3	—	5.1, 5.2
2 Політика безпеки інформаційної системи	—	—	1.1, 1.2	5.2, 5.3	*.3.1.1	3	—	5.2, 5.3
3 Керування інформаційною безпекою	4.1.1, 4.1.2	—	1.1, 1.2	6	*.3.1.1	4	2.1	6
4 Розподіл обов'язків	4.1.3	—	1.3	2.4, 2.5, 3	*.3.1.1	4	2.1	2.4, 2.5, 3
5 Організація інформаційної безпеки	4.1	—	1.2	3.5	—	4	2.2	3.5
6 Визначення і оцінювання цінностей	5	—	2.2	7.1	—	5.6, 7.1	5.1	7.1
7 Затвердження інформаційних систем	4.1.4	—	—	8	5	—	6.7	8, 9
<sup>1</sup> * Позначає довільне число між 6 та 11.								

**Таблиця 8.1.2** — Перевіряння узгодженості безпеки

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Відповідність політиці інформаційної безпеки та засобам захисту	12.2	—	1.2	10.2.3	—	10.2	7.1, 7.2	9.4, 10.2.3

Кінець таблиці 8.1.2

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
2 Відповідність правовим та регуляторним вимогам.	12.1	—	3.1, 3.2	6.3, 10.2.3	6.3.11	8.18, 10.2	8.1	1.5, 2.9, 6.3, 10.2.3

Таблиця 8.1.3 — Реагування на порушення

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Звітвання про порушення безпеки	6.3.1	—	M2	12	—	10.4	—	12
2 Звітвання про слабкості безпеки	6.3.2	—	M2	12	—	10.4	—	12
3 Звітвання про збої програмного забезпечення	6.3.3	—	M2	12	—	10.4	—	12
4 Керування порушеннями	8.1.3	—	M2	12	—	10.4	—	18.1.3

Таблиця 8.1.4 — Персонал

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Засоби захисту постійного та тимчасового штату	6.1	—	3.2, M3	10.1	*.3.9	9.2	4.1, 2.2	10.1
2 Засоби захисту персоналу, що працює за контрактами	6.1	—	—	10.3	*.3.9	9.2	4.1, 2.2	10.3
3 Усвідомлення безпеки та навчання	6.2	—	1.2, M3	13, 10.1.4	*.3.9	9.1	4.2, 2.2	13, 10.1.4
4 Дисциплінарний процес	6.3.5	—	3.2, M3	—	*.3.9	9.2.6	2.2.1	13.1
<sup>1</sup> * Позначає довільне число між 6 та 11.								



Таблиця 8.1.5 — Питання експлуатації

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Керування конфігурацією та змінами	8.2, 10.5	—	—	14.3, 8.4.1	—	7.4	9	14.3, 8.4.1, 8.4.4
2 Керування потужностями	8.2.1	—	—	—	—	—	—	—
3 Документація	8.1.1, 8.6.3	—	M2	14.6	—	8.4.6, 8.5.7, 8.7	—	14.6
4 Обслуговування	7.2.4	—	M2	14.7	*.3.6	8.1.4, 8.10.5, 10.1	6.5	14.7
5 Моніторинг змін, що стосуються безпеки	—	—	1.2	7.3.3	—	7.4, 8.1.3, 8.2.5, 8.3.7	6.7	7.3.3, 8.4.4
6 Результати аудиту та ведення журналів	8.4	—	M2	18	—	7.3, 8.1.8, 8.2.10, 8.9.5	6.7	(18)
7 Тестування безпеки	—	—	M2	8.4.3	—	8.3.5	6.7, 3	8.4.3
8 Контроль носіїв інформації	8.6	—	8, M2	14.5	*.3.5	8.4 — 8.14	5	14.5
9 Гарантоване вилучення інформації	—	—	M4	—	—	8.1.9	6.3, 5	14.5.7
10 Розподіл обов'язків	8.1.4	—	M2	—	—	—	—	10.1.1
11 Правильне використання програмного забезпечення	12.1.2	—	M2	—	*.3.8	8.3	6.3	14.2
12 Контроль змін програмного забезпечення	10.5.1, 10.5.3	—	M2	—	*.3.8	8.3.7	6.3	8.4.4, 14.2

<sup>1</sup> \* Позначає довільне число між 6 та 11.

Таблиця 8.1.6 — Планування неперервності бізнесу

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Стратегія неперервності бізнесу	11.1.1, 11.1.2	—	3.3, M6	11.2, 11.3, 11.4	*.3.3	8.19, 8.1.7, 8.4.5, 8.5.5, 8.6.5, 8.7.5, 8.8.3, 8.19	7.3, 7.4, 7.5	11.2, 11.3, 11.4

Кінець таблиці 8.1.6

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
2 План неперервності бізнесу	11.1.3, 11.1.4	—	3.3, M6	11.5	*.3.3	8.19, 8.1.7, 8.4.5, 8.5.5, 8.6.5, 8.7.5, 8.8.3, 8.19	—	11.5
3 Тестування та оновлення плану неперервності бізнесу	11.1.5	—	3.3, M6	11.6	*.3.3		—	11.6
4 Резервування	8.4.1	—	3.4	14.4	*.3.2.4	—	7.1, 7.2	14.4

<sup>1</sup> \* Позначає довільне число між 6 та 11.

Таблиця 8.1.7 — Фізична безпека

	Практичні правила керування інформаційною безпекою	Стандарт базової безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист для інформаційних систем охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Матеріальний захист	7.1	—	4.1, 4.3, M1	15.1	*.3.1.2	8.1.1, 8.6.2, 8.9.1	3.1, 3.4, 4	15.1
2 Протипожежний захист	7.2.1	—	—	15.2	*.3.1.4	8.1.1, 8.6.2, 8.9.1	3.1, 3.2, 7.5	15.2
3 Захист від води/рідини	7.2.1	—	M2	15.5	*.3.1.4	8.1.1, 8.6.2, 8.9.1	7.5	15.5
4 Захист від стихійних лих	7.2.1	—	M2	15.4	*.3.1.4	8.1.1, 8.6.2, 8.9.1	7.5	15.4
5 Захист від крадіжок	7.1	—	1.2	15.1	*.3.1.3	8.1.1, 8.6.2, 8.9.1	3.3, 3.4, 4	15.1
6 Електричне живлення та кондиціонування повітря	7.2.2	—	M2	15.6	*.3.4	8.1.1, 8.6.2, 8.9.1	3.2, 7.3	15.6
7 Прокладання кабелю	7.2.3	—	4.2, M1	—	—	8.1.1, 8.6.2, 8.9.1	8.2	15, 15.1, 15.7

<sup>1</sup> \* Позначає довільне число між 6 та 11.

## 8.2 Специфічні засоби захисту інформаційної системи

У кінці цього підрозділу у таблицях, що стосуються кожної підгрупи показано, де можна знайти додаткову інформацію про згадані категорії засобів захисту.

### 8.2.1 Ідентифікація та автентифікація (I&A)

Ідентифікація є засобом, яким користувач надає системі заявлену ідентичність. Автентифікація — це метод визначення дійсності цієї заявки. Нижченаведені способи — це приклади, як досягнути I&A (можливі інші способи класифікації механізмів I&A).

1 I&A на основі інформації, якою володіє користувач

Паролі є найтипівішим способом забезпечення I&A на основі того, чим володіє користувач

і що пов'язано з процесом ідентифікації користувача. Призначення паролів та їхню регулярну зміну треба контролювати. Якщо користувачі вибирають паролі самостійно, вони повинні знати про загальні правила створення і поводження з паролями. В цьому питанні може допомогти програмне забезпечення, наприклад, для обмеження використання простих чи шаблонних паролів та символів. Якщо необхідно чи бажано, копії паролів слід захищати, щоб дозволити авторизований доступ, якщо користувач не має в розпорядженні чи забув свій пароль. I&A на основі інформації, якою володіє користувач, також може використовувати криптографічні методи чи протоколи автентифікації. Цей тип ідентифікації та автентифікації також може бути використаний для віддаленої I&A.

#### **2 I&A на основі того, чим володіє користувач**

Об'єктами, якими володіє користувач для цілей I&A, можуть бути модулі пам'яті та інтелектуальні модулі. Звична реалізація таких модулів пам'яті — магнітний матеріал на звороті кредитної картки. Автентифікація забезпечується на основі того, чим володіє користувач (картка) та того, що він знає (PIN-код). Типовими прикладами інтелектуальних модулів є смарт-картки.

#### **3 I&A на основі того, ким є користувач**

Технології біометричної автентифікації використовують унікальні характеристики чи риси людини для визначення її особистості. Це можуть бути відбитки пальців, форма руки, знімок сітківки ока, а також голос чи письмовий підпис. Відповідні деталі треба безпечно зберігати на смарт-картках чи в системі.

### **8.2.2 Контролювання логічного доступу та аудит**

Засоби захисту в цій області реалізують для:

- обмеження доступу до інформації, комп'ютерів, мереж, додатків, системних ресурсів, файлів та програм, і

- запису деталей помилок та дій користувача в журнали аудиту та аналізування записаних деталей для виявлення порушень безпеки і реагування на них відповідним чином.

Звичний метод для впровадження контролю доступу — це використання списків контролю доступу, що визначають, до яких файлів, ресурсів тощо користувачу дозволено доступ, і які форми цей доступ може мати. Засоби захисту в сфері контролю логічного доступу та аудиту наведено нижче.

#### **1 Політика контролю доступу**

Для кожного користувача чи групи користувачів треба чітко визначити політику контролю доступу. Ця політика має надавати права доступу відповідно до ділових потреб, таких як доступність, продуктивність та принцип "необхідного знання". Загальна ідея така: "максимальна кількість прав, яка вважається необхідною, мінімальна кількість прав, яка вважається можливою". Під час призначення прав доступу потрібно брати до уваги підхід організації до безпеки (наприклад, відкритий чи обмежувальний) та способи забезпечення потреб організації і прийнятності системи для користувача.

#### **2 Доступ користувачів до комп'ютерів**

Контроль доступу до комп'ютерів застосовують для запобігання будь-якого неавторизованого доступу до комп'ютера. Має бути можливою ідентифікація та перевіряння ідентичності кожного авторизованого користувача та ведення журналів успішності чи неуспішності спроби. Контроль доступу до комп'ютерів можна посилити паролями чи будь-яким іншим методом I&A.

#### **3 Доступ користувачів до даних, служб та програм**

Контроль доступу треба застосовувати для захисту даних чи служб на комп'ютері чи в мережі від несанкціонованого доступу. Це може бути зроблено за допомогою відповідних механізмів ідентифікації та автентифікації (див. 8.2.1), відповідних інтерфейсів між мережними службами та конфігурації мережі, яка гарантує лише авторизований доступ до інформаційних служб (обмежувальний розподіл прав). Для запобігання несанкціонованому доступу до програм потрібно запроваджувати рольовий контроль доступу, що дозволяє доступ відповідно до ділових обов'язків користувача.

#### **4 Перегляд і оновлення прав доступу**

Усі права доступу, що надаються користувачам, мають регулярно переглядатися та оновлюватися, якщо потреби безпеки чи ділові потреби доступу змінилися. Права привілейованого доступу треба переглядати частіше, щоб уникнути їх нецільового використання. Права доступу негайно скасовують, якщо вони більше не потрібні.

#### **5 Журнали аудиту**

Усю роботу по супроводженню IT треба записувати в журналі, а ці журнали регулярно перевіряти; це охоплює успішні та неуспішні спроби входу в систему, ведення журналу доступу до даних,

функцій системи тощо. Також необхідно вести журнали збоїв і регулярно переглядати ці журнали. Всі ці дані потрібно використовувати відповідно до законодавства про захист даних та приватного життя, наприклад, їх можна зберігати тільки обмежений строк та використовувати тільки для виявлення порушень захисту.

### 8.2.3 Захист від зловмисного коду

Зловмисний код може потрапляти до систем через зовнішні сполучення, а також через файли та програмне забезпечення, занесені на переносних дисках. Якщо не реалізовані відповідні засоби захисту, цей код можна не виявити, доки він не призвів до пошкоджень. Зловмисний код може призводити до компрометації безпеки засобів захисту (наприклад, перехват і розкриття паролів), незловмисного розкриття інформації, внесення незловмисних змін до інформації, втрати цілісності системи, руйнування інформації, та (або) несанкціонованого використання системних ресурсів.

Зловмисний код може бути таких видів:

- віруси,
- черв'яки, та
- троянські коні.

Переносниками зловмисного коду є:

- програми, що запускаються,
- файли даних (що містять макроси, наприклад, текстові документи чи таблиці),
- активний вміст сторінок Інтернету.

Зловмисний код може поширюватись через:

- дискети,
- інші знімні носії інформації,
- електронну пошту,
- мережі,
- завантаження (по каналах зв'язку).

Зловмисний код може бути введений внаслідок зловмисних дій користувача чи у разі взаємодії системних рівнів, що може бути невидимим для користувачів. Захистити від зловмисного коду можна, використавши засоби захисту, наведені нижче.

#### 1. Сканери

Різні форми зловмисного коду можуть бути виявлені та видалені спеціальним сканувальним програмним забезпеченням та програмами перевіряння цілісності. Сканери можуть працювати в закритому чи відкритому режимах. Робота сканера у відкритому режимі забезпечує активний захист, тобто виявлення (і, можливо, видалення) зловмисного коду перед тим, як відбулося зараження та інформаційній системі заподіяна шкода. Є сканери для окремих комп'ютерів, робочих станцій, файлових серверів, серверів електронної пошти та брандмауерів. Однак, користувачі та адміністратори мають знати про те, що на сканери не можна покладатися у виявленні всіх зловмисних кодів (чи навіть всього коду певного типу), оскільки постійно з'являються нові форми зловмисного коду.

#### 2. Програми перевіряння цілісності

Зазвичай, для доповнення засобів захисту, що забезпечується сканерами, потрібні інші форми засобів захисту. Наприклад, контрольні суми можна використовувати для перевіряння того, чи була програма модифікована. Програми перевіряння цілісності мають бути складовою частиною технічних засобів захисту від зловмисного коду. Ця техніка може бути використана тільки для файлів даних та програм, що не зберігають інформацію про статус для подальшого використання.

#### 3. Контроль за обігом переносних носіїв інформації

Неконтрольований обіг носіїв інформації (особливо дискет) може призвести до зростання ризику введення зловмисного коду в інформаційні системи організації. Контроль за обігом носіїв може бути досягнуто використанням:

- спеціального програмного забезпечення,
- процедурних засобів захисту (див. нижче).

#### 4 Процедурні засоби захисту

Треба розробити настанови для користувачів та адміністраторів, що окреслюють процедури та правила мінімізації проникнення зловмисного коду. Такі настанови мають стосуватися питання завантаження ігор та інших виконуваних програм, використання різних видів Інтернет-служб та

важливих файлів різних типів. За необхідності, треба виконувати незалежний перегляд вихідного чи виконуваного коду. Треба запроваджувати навчання, що стосуються питань безпеки, та дисциплінарні заходи і відповідні процедури за недотримання задокументованих процедур і правил запобігання зловмисному коду.

#### **8.2.4 Керування мережею**

Ця сфера охоплює теми планування, експлуатації та адміністрування мереж. Правильна конфігурація та адміністрування мереж є ефективним методом зменшення ризиків. Зараз ISO працює над декількома документами, що містять подальшу інформацію про детальні засоби захисту для забезпечення мережної безпеки. Засоби захисту в сфері керування мережею наведено нижче.

##### **1 Процедури експлуатації**

Запровадження процедур експлуатації та обов'язків необхідне для забезпечення правильного та безпечного функціонування мереж. Вони містять документацію експлуатації та запровадження процедур реагування у разі порушення безпеки (див. також 8.1.3).

##### **2 Планування системи**

Для забезпечення надійного функціонування та адекватних мережних потужностей необхідне розвинене планування, підготовка та моніторинг (охоплюючи статистику завантаження). Для нових систем треба застосовувати критерій прийняття, треба здійснювати контроль за змінами та реагування на них (див. також 8.1.5).

##### **3 Конфігурація мережі**

Прийнятна конфігурація мережі є істотною для її надійного функціонування. Вона містить стандартизований підхід до конфігурації серверів в організації, та, що дуже важливо, хорошу документацію. Більше того, треба пересвідчитися, що сервери, використовувані для спеціальних цілей, використовують тільки для цих цілей (наприклад, ніякі інші задачі не запускаються на брандмауері), і що є достатній захист від збоїв.

##### **4 Відокремлення мережі**

Для мінімізації ризиків та можливостей зловживання в мережі під час її експлуатації, ділові зони, що мають справу з критичними діловими питаннями та інформацією, треба відокремлювати логічно чи фізично. Також засоби розроблення треба відокремлювати від засобів, що експлуатують.

##### **5 Моніторинг мережі**

Для визначення слабких місць у наявній конфігурації мережі треба здійснювати моніторинг мережі. Він дозволяє перебудовувати структуру мережі, за допомогою аналізування робочого навантаження та допомагає визначити нападників.

##### **6 Виявлення вторгнень**

Спроби вторгнень до систем чи мереж та успішний несанкціонований вхід треба виявляти так, щоб організація могла відреагувати відповідним та ефективним чином.

#### **8.2.5 Криптографія**

Криптографія — це математичні методи перетворення даних для забезпечення безпеки. Її можна застосовувати для багатьох різних цілей в інформаційній безпеці, наприклад, криптографія може допомогти забезпечити конфіденційність та (або) цілісність даних, неспростовність і посилені методи ідентифікації та автентифікації. Застосовуючи криптографію, треба подбати про те, щоб дотримувалися всі правові та регуляторні вимоги в цій сфері. Один з найважливіших аспектів криптографії — адекватна система керування ключами, що описана детальніше в ISO/IEC 11770-1. Подальша інформація про класи застосування криптографії також може бути знайдена в додатку C ISO/IEC 11770-1. Використання криптографії для ідентифікації та автентифікації описано в 8.2.1. Послуги штемпелювання часу можна використовувати для підтримування окремих програм криптографічних засобів захисту. Різні способи використання криптографії описано нижче.

##### **1 Захист конфіденційності даних**

В обставинах, коли важливо зберігати конфіденційність, тобто коли інформація є надзвичайно чутливою, треба розглядати засоби захисту, що зашифровують інформацію для зберігання чи передавання мережею. Під час вирішення питання про використання засобів шифрування треба брати до уваги:

- відповідні державні закони та норми,
- вимоги до керування ключами та труднощі, які треба подолати для гарантування того, що справжні поліпшення безпеки досягаються без створення нових вразливостей, та

— прийнятність використання механізмів шифрування для розгортання та рівень необхідного захисту.

## 2 Захист цілісності даних

За обставин, коли важливим є цілісність даних, що зберігаються чи оброблюються, для захисту цих даних треба розглянути геш-функції, цифрові підписи та (або) засоби забезпечення цілісності. Засоби захисту цілісності (наприклад, використання так званих кодів автентифікації повідомлень (MAC)) надають захист від випадкової чи зловмисної зміни, долучення чи вилучення інформації. Засоби цифрових підписів можуть забезпечувати захист, схожий до засобів цілісності повідомлень, але також мають властивості, що дозволяють уможливити неспростовність. У разі вирішення питання про використання цифрових підписів чи інших засобів забезпечення цілісності, треба брати до уваги:

- відповідні державні закони та норми,
- відповідну інфраструктуру відкритих ключів,
- вимоги до керування ключами та труднощі, які потрібно подолати для гарантування того, що справжнього поліпшення безпеки досягають без створення нових вразливостей.

## 3 Неспростовність

Методи криптографії (наприклад, засновані на використанні цифрових підписів) можуть бути використані для повідомлень, комунікацій та транзакцій з метою підтвердження чи спростування відправлення, передавання, подання, доставлення, оповіщення про отримання тощо.

## 4 Автентичність даних

У ситуаціях, коли є важливою автентичність даних, для підтвердження достовірності даних може бути використаний цифровий підпис. Ця необхідність проявляється особливо, коли використовуються дані, на які посилає третя сторона, або коли велика кількість людей залежить від точності даних джерел, на які посилаються. Цифрові підписи також можна використовувати для підтвердження факту, що дані створені чи передані певною особою.

## 5 Керування ключами

Керування ключами охоплює технічні, організаційні та процедурні аспекти, необхідні для використання будь-якого механізму криптографії. Метою керування ключами є безпечне адміністрування та керування криптографічними ключами та пов'язаною з ними інформацією. Керування ключами охоплює генерування, реєстрування, сертифікування, дереєстрування, поширення, встановлення, зберігання, архівування, відгук, виведення та знищення ключового матеріалу. На додаток, важливо розробляти систему керування ключами так, щоб зменшити ризик компрометування ключа та використання ключа неуповноваженими особами. Процедури керування ключами залежать від використання алгоритму наміру щодо використання ключів та політики безпеки. Для одержання більшої інформації про керування ключами дивіться також ISO/IEC 11770-1.

Таблиця 8.2.1 — Ідентифікація та автентифікація (I&A)

	Практичні правила керування інформаційною безпекою	Базовий стандарт безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист інформаційних систем для охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 I&A на основі інформації, якою володіє користувач	9.2.3, 9.3.1, 9.4, 9.5.1	4.2.1, 5.2.1, додаток A	M4	16.1	*3.2.1	7.2.1, 7.2.2	6.2	16.1
2 I&A на основі того, чим володіє користувач			—	16.2	*3.2.1		6.2	16.2
3 I&A на основі того, ким є користувач			—	16.3	*3.2.1		6.2	16.3

<sup>1</sup> \* Позначає довільне число між 6 та 11.

Таблиця 8.2.2 — Контролювання логічного доступу та аудит

	Практичні правила керування інформаційною безпекою	Базовий стандарт безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист інформаційних систем для охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Політика контролю доступу	9.1	—	M2	17.1, 17.2, 17.3	*.3.2.1	7.2, 8.1.2, 8.2.2, 8.4.1	6.4	17.1, 17.2, 17.3
2 Доступ користувачів до комп'ютерів	9.2, 9.3, 9.5	4.2.4, 5.2.4, додаток A	M4		*.3.2.1		6.2, 3.3	
3 Доступ користувачів до даних, служб та програм	9.4, 9.6		M4		*.3.2.1		6.4	
4 Перегляд і оновлення прав доступу	9.1, 9.2.4	—	M2	17.4	*.3.2.1		—	17.4
5 Журнали аудиту	9.7	—	M4	18	*.3.2.2	7.3, 8.2.10	6.7	18
<sup>1</sup> * Позначає довільне число між 6 та 11.								

Таблиця 8.2.3 — Захист від зловмисного коду

	Практичні правила керування інформаційною безпекою	Базовий стандарт безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист інформаційних систем для охорони здоров'я <sup>1</sup>	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Сканери	8.3	—	M4	—	*.3.10	8.3.11, 8.3.16	7.4	4.6, 5.2.1, 6.4, 8.4.4, 11
2 Програми перевіряння цілісності	8.3	—	M4	—	—	8.3.11, 8.3.16	7.4	—
3 Контроль за обігом переносних носіїв інформації	7.3.2	—	—	—	—	—	—	—
4 Процедурні засоби захисту	8.3	—	M4	—	*.3.10	8.3.11, 8.3.16	7.4	6.2.2, 9.3, 12, 14.2
<sup>1</sup> * Позначає довільне число між 6 та 11.								

Таблиця 8.2.4 — Керування мережею

	Практичні правила керування інформаційною безпекою	Базовий стандарт безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист інформаційних систем для охорони здоров'я	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Методика експлуатації	8.5.1	—	M2	—	—	8.2, 8.3	8.2	14.6
2 Планування системи	8.2	—	M2, M4	8.4	—		6.1	8.4
3 Конфігурація мережі	—	—	M4	—	—		9, 6.1	14.3
4 Відокремлення мережі	9.4.6	—	M2	—	—	—	3.1	—
5 Моніторинг мережі	9.7	—	M2	18.1.3	—	8.2.7	—	18.1.3
6 Виявлення вторгнень	—	—	—	18.1.3	—	—	6	18.1.3

Таблиця 8.2.5 — Криптографія

	Практичні правила керування інформаційною безпекою	Базовий стандарт безпеки ETSI — Функції та механізми	Довідник з базового захисту IT	Посібник з комп'ютерної безпеки NIST	Категоризація безпеки та захист інформаційних систем для охорони здоров'я	Настанова з інформаційної безпеки TC 68	Рекомендації для комп'ютерних робочих станцій	Канадський посібник з безпеки інформаційних технологій
1 Захист конфіденційності даних	10.3.2	4.2.2, 5.2.2, додаток A	M4	19.5.1	—	8.23	8.1	19.5.1
2 Захист цілісності даних	10.3.3	4.2.3, 5.2.3, додаток A	M4	19.5.2	—	8.23	8.1	19.5.2
3 Неспровтовність	10.3.4	4.2.6, 5.2.6, додаток A	—	19.2.3	—	8.23	8.1	19.2.3
4 Автентичність даних	10.3.2	4.2.3, 5.2.3, додаток A	M4	19.5.2	—	8.23	8.1	19.5.2
5 Керування ключами	10.3.5	4.2.5, 5.2.5, додаток A	—	19.3	—	8.23	8.1	19.3



## 9 БАЗОВИЙ ПІДХІД: ВИБІР ЗАСОБІВ ЗАХИСТУ ВІДПОВІДНО ДО ТИПУ СИСТЕМИ

Як описано в розділі 8, є два різні набори засобів захисту, механізмів та (або) процедур, які можна застосовувати для захисту інформаційних систем. З одного боку, є доволі багато організаційних категорій засобів захисту, які є загальноприйнятими для кожної інформаційної системи за конкретних обставин (як описано в 8.1), незалежно від окремих компонентів. Вибір цих засобів захисту описано в 9.1. Внаслідок їх загальної застосовності, засоби, які належать до цих категорій треба завжди розглядати. До того ж, багато з них є недорогими для впровадження, оскільки вони стосуються організаційних структур та процедур.

З іншого боку, є специфічні засоби захисту інформаційної системи (як описано в 8.2) — вибір цих засобів захисту залежить від типу та характеристик інформаційної системи, що розглядається. Вибір цих засобів описано в 9.2.

Звичайно, можливо, що одна чи більше з цих категорій або специфічних засобів захисту не є застосовними до інформаційної системи. Наприклад, шифрування може не бути необхідним, якщо відправлена чи отримана інформація не потребує конфіденційності, а цілісність може бути перевірена іншим чином. Знову ж таки, детальніший вибір можна зробити, тільки враховуючи наступну інформацію (див. розділи 10 та 11).

Після того, як визначені всі типи засобів захисту, застосовні до обговорюваної інформаційної системи, подальша інформація щодо цих типів засобів захисту та специфічних засобів може бути отримана з розділу 8 та одного чи більше документів, наведених у додатках А—Н (посилання на розділ 8 наведено в таблиці в кінці розділу 9). Перед реалізуванням вибраних засобів захисту треба ретельно перевірити, чи їх немає серед наявних та (або) запланованих (див. 7.3).

Використання детальнішого аналізування для вибору додаткових засобів розглянуто нижче (див. розділи 10 та (або) 11). Якщо засоби захисту вибрані відповідно до інших критеріїв (наприклад базові та додаткові засоби), остаточний набір засобів для впровадження треба робити обережно. Після перегляду декількох інформаційних систем, потрібно розглянути, чи можна запровадити базову безпеку для всієї організації (розділ 12).

Інша можливість вибору засобів захисту без детального розгляду — це застосування баз, пов'язаних з конкретним використанням. Наприклад, доступні базові довідники для телекомунікацій, охорони здоров'я, банківської справи (див. додатки В, Е та F) і багато інших. У разі використання цих довідників, наприклад, можливо перевірити наявні чи заплановані засоби на відповідність рекомендованим. Але перед вибором того, які засоби захисту треба впроваджувати, корисно розглянути потреби та проблеми безпеки.

### 9.1 Засоби захисту загального застосування

Категоріями загального застосування засобів захисту є:

- керування інформаційною безпекою та політики безпеки (8.1.1),
- перевіряння узгодженості безпеки (8.1.2),
- реагування на порушення (8.1.3),
- персонал (8.1.4),
- питання експлуатації (8.1.5),
- планування неперервності бізнесу (8.1.6) та
- фізична безпека (8.1.7).

Засоби захисту, які належать до цих категорій формують основу успішного керування інформаційною безпекою, їх не треба недооцінювати. Також важливо забезпечити взаємодію цих засобів з більш технічними засобами, що розглядаються нижче. Організація визначає обсяги робіт у цих сферах, залежно від її потреб, проблем (див. розділ 10) та доступних ресурсів.

Звичайно, багато інших категорій засобів захисту застосовні в більшості випадків, але спосіб реалізації зазвичай є відповідним конкретним обставинам (наприклад, засоби, які забезпечують контроль доступу для мережі відрізняються від тих засобів, що забезпечують контроль доступу для автономного комп'ютера).

Коли засоби захисту вибирають з категорій загально застосовних засобів, корисно розглядати розмір організації так само, як потреби безпеки, оскільки він впливає на межі, в яких реалізуються ці засоби захисту. Наприклад, маленька організація не буде мати ні потреби, ні персоналу для створення комітету інформаційної безпеки, проте має бути хтось, хто виконує ці функції. Тому всі засоби захисту, наведені в 8.1, мають бути відповідно зважені, коли б це не знадобилося.

## 9.2 Специфічні засоби захисту інформаційної системи

На додаток до засобів захисту загального застосування, для кожного відповідного типу системного компонента треба вибирати специфічні засоби захисту системи. Нижченаведена таблиця дає приклад того, як починати процес вибору специфічних засобів системи. В цьому прикладі 'X' означає засоби, що мають реалізовуватись за нормальних обставин, та '(X)' означає засоби, що можуть бути необхідними за деяких обставин. Процес вибору засобів захисту буде продовжено під час розгляду описів засобів захисту, наведено у 8.2, та, за потреби, з документів базових засобів захисту, наведених у додатках A—H.

	Автономна робоча станція	Робоча станція (клієнт без спільних ресурсів), під'єднана до мережі	Сервер чи робоча станція зі спільними ресурсами, під'єднана до мережі
<b>I&amp;A</b>			
I&A на основі інформації, якою володіє користувач	X	X	X
I&A на основі дечого, чим володіє користувач	X	X	X
I&A на основі того, ким є користувач	(X)	(X)	(X)
<b>Контроль логічного доступу та аудит</b>			
Політика контролю доступу			X
Доступ користувачів до комп'ютерів	X	X	X
Доступ користувачів до даних, служб та програм	X	X	X
Перегляд і оновлення прав доступу			X
Журнали аудиту	X	X	X
<b>Зловмисний код</b>			
Сканери	X	X	X
Програми перевіряння цілісності	X	X	X
Контроль за обігом переносних носіїв інформації	X	X	X
Процедурні засоби захисту	X	X	X
<b>Керування мережею</b>			
Методика експлуатації			X
Планування системи			X
Конфігурація мережі			X
Відокремлення мережі			X
Моніторинг мережі			X
Виявлення вторгнень			X
<b>Криптографія</b>			
Захист конфіденційності даних	(X)	(X)	(X)
Захист цілісності даних	(X)	(X)	(X)

Кінець таблиці

	Автономна робоча станція	Робоча станція (клієнт без спільних ресурсів), під'єднана до мережі	Сервер чи робоча станція зі спільними ресурсами, під'єднана до мережі
Неспростовність		(X)	(X)
Автентичність даних	(X)	(X)	(X)
Керування ключами	(X)	(X)	(X)

## 10 ВИБІР ЗАСОБІВ ЗАХИСТУ ВІДПОВІДНО ДО ПРОБЛЕМ ТА ЗАГРОЗ БЕЗПЕЦІ

Вибір засобів захисту відповідно до проблем та загроз безпеці, описаний в цьому розділі, можна використовувати таким чином.

1. Перший крок — визначити та оцінити проблеми безпеки. Треба розглянути вимоги до конфіденційності, цілісності, доступності, спостережності, автентичності та надійності. Міцність та кількість вибраних засобів захисту має відповідати оціненим проблемам безпеки.

2. Другий — для кожної проблеми безпеки визначають типові загрози і для кожної загрози пропонують засоби захисту інформаційної системи, що розглядається. Різні типи інформаційних систем описано в підрозділі 7.1, можливі засоби захисту наведено в підрозділах розділу 8. У такий спосіб можливо задовольнити специфічні потреби безпеки та досягнути захисту там, де він дійсно необхідний.

### 10.1 Оцінювання проблем безпеки

Для ефективного вибору прийнятих засобів захисту, необхідно розуміти проблеми безпеки підтримуваних ділових операцій інформаційною системою, що розглядається. За допомогою визначення проблем безпеки, беручи до уваги відповідні загрози, що можуть призвести до цих проблем, засоби захисту треба вибирати, як описано в 10.2—10.5.

Якщо оцінювання, проведено згідно з положеннями цього підрозділу виявляє дуже великі проблеми безпеки, рекомендується деталізованіший підхід для визначання прийнятного захисту. Допомогу з цього питання можна знайти в розділі 11.

Проблеми безпеки мають містити:

- втрату конфіденційності,
- втрату цілісності,
- втрату доступності,
- втрату спостережності,
- втрату автентичності та
- втрату надійності.

Оцінювання має охоплювати саму інформаційну систему, інформацію, що зберігається чи обробляється на ній, та ділові операції, які вона виконує. Це оцінювання визначає цілі вибраних засобів захисту. Різні частини інформаційної системи або інформація, що зберігається чи обробляється, можуть мати різні проблеми безпеки. Важливо пов'язувати проблеми безпеки безпосередньо з цінностями, оскільки це впливає на загрози, які можуть з'являтися, і, таким чином, на вибір засобів захисту.

Значимість проблем безпеки може бути оцінена залежно від того, чи порушення безпеки спричинює серйозні uszkodження ділової діяльності, або ж тільки завдає легкої шкоди, чи не впливає зовсім. Наприклад, якщо конфіденційна інформація компанії обробляється інформаційною системою, несанкціоноване розкриття цієї інформації конкуренту може дозволити йому зробити дешевші пропозиції і, таким чином, заподіяти серйозні збитки бізнесу організації. З іншого боку, якщо інформація, яка доступна широкому загалу, обробляється інформаційною системою, несанкціоноване розкриття не заподіє ніяких збитків. Розгляд можливих загроз (див. 10.2—10.5) може допомогти з'ясувати проблеми безпеки. Оцінювання, описане нижче, треба проводити окремо для кожної цінності, оскільки проблеми безпеки для різних цінностей можуть бути різними. Однак, якщо є достатні знання з проблем безпеки, цінності з однаковими чи схожими діловими потребами та проблемами безпеки можуть бути об'єднані в групи.

Якщо інформація, оброблювана системою, є різнотипною, різні її типи можуть вимагати окремого розгляду. Захист, що надається інформаційній системі, має бути достатнім для всіх типів оброблюваної інформації. Таким чином, якщо певна інформація потребує високого рівня безпеки, всю систему треба захищати належним чином. У випадку, якщо кількість інформації з великими потребами безпеки незначна, є сенс розглянути перенесення цієї інформації в іншу систему, якщо це не заважає діловим процесам.

Коли всі можливі втрати конфіденційності, цілісності, доступності, спостережності, автентичності та надійності визначені як можлива причина тільки незначної втрати, достатню безпеку системи, що розглядається, може забезпечувати підхід, описаний в підрозділі 10.2. Коли будь-яка з цих втрат визначена як можлива причина серйозних збитків, треба оцінити, чи потрібно підбирати засоби захисту, додаткові до зазначених у підрозділах 10.2—10.5. Пропозиції детальнішого оцінювання та вибору засобів захисту відповідно до результатів цих оцінювань наведено в ISO/IEC TR 13335-3 та в розділі 11. Проте пропонувані засоби, починаючи із зазначених у 10.2, можуть бути використані як основа для удосконалювання вибору.

#### **10.1.1 Утрата конфіденційності**

Розглянемо, які збитки можуть виникнути внаслідок втрати конфіденційності цінностей, що розглядаються (зловмисної чи незловмисної). Наприклад, втрата конфіденційності може призвести до:

- втрати суспільної довіри чи погіршення репутації,
- судової відповідальності, включаючи відповідальність за порушення законодавства про захист даних,
- несприятливі наслідки організаційної політики,
- загрози власній безпеці та
- фінансових втрат.

Відповідно до відповідей на поставлені вище питання, має бути вирішено, чи будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

#### **10.1.2 Утрата цілісності**

Розглянемо, які збитки можуть виникнути внаслідок втрати цілісності згаданих цінностей (зловмисної чи незловмисної). Наприклад, втрата цілісності може призвести до:

- прийняття невірних рішень,
- обману,
- порушення ділових функцій,
- втрати суспільної довіри чи погіршення репутації,
- фінансових втрат та
- судової відповідальності, включаючи відповідальність за порушення законодавства про захист даних.

Залежно від відповідей на поставлені вище питання, треба вирішити, чи будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

#### **10.1.3 Утрата доступності**

Розглянемо, які збитки можуть виникнути внаслідок довготермінової втрати доступності до програм чи доступності до інформації, тобто переривання яких ділових функцій призведе до невчасної відповіді на запит чи невчасного виконання. Також має бути розглянута крайня форма втрати доступності, остаточна втрата даних та (або) фізичне руйнування апаратного чи програмного забезпечення. Наприклад, втрата доступності до критичних програм чи доступності до критичної інформації може призвести до:

- прийняття невірних рішень,
- неможливості виконувати ризиковані задачі,
- втрати суспільної довіри чи погіршення репутації,
- фінансових втрат,
- судової відповідальності, включаючи відповідальність за порушення законодавства про захист даних, недотримання термінів виконання, вказаних в контракті, та
- суттєвих затрат на відновлення.

Треба зазначити, що величина збитків внаслідок втрати доступності може досить сильно відрізнятись у різні періоди часу. Коли це дійсно так, то доречно розглянути всі збитки, що можуть виникнути в ці різні періоди часу, та оцінити їх для кожного періоду як значні, незначні чи нульові (ця інформація буде використовуватись в виборі засобів захисту).

Залежні від наданих відповідей на поставлені вище питання, треба вирішити, чи будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

#### **10.1.4 Утрата спостережності**

Розглянемо, які збитки можуть виникнути внаслідок втрати спостережності за користувачами системи чи суб'єктами (наприклад, програмами), що виконують доручення користувача. Цей розгляд також має охоплювати автоматично згенеровані повідомлення, які можуть стати причиною проведення дії. Наприклад, втрата спостережності може призвести до:

- маніпуляції системою з боку користувачів,
- обману,
- індустріального шпіонажу,
- дій, що не прослідковуються,
- помилкових обвинувачень та
- судової відповідальності, включаючи відповідальність за порушення законодавства про

захист даних.

Залежно від відповідей на поставлені вище питання, має бути вирішено, чи будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

#### **10.1.5 Утрата автентичності**

Розглянемо, які збитки можуть виникнути внаслідок втрати автентичності даних та повідомлень, незалежно від того, хто їх використовує: люди чи система. Це особливо важливо в розподілених системах, де прийняті рішення поширюються на широкий загал, чи у разі використання довідкової інформації. Наприклад, втрата автентичності може призвести до:

- обману,
- використання в правильному процесі неправильних даних, що призводить до неправильного результату,
- маніпуляції організацією з боку сторонніх осіб,
- індустріального шпіонажу,
- помилкових обвинувачень та
- судової відповідальності, включаючи відповідальність за порушення законодавства про

захист даних.

Залежно від наданих відповідей на поставлені вище питання, має бути вирішено, чи будуть загальні збитки, що можуть виникнути внаслідок втрати конфіденційності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

#### **10.1.6 Утрата надійності**

Розглянемо, які збитки можуть виникнути внаслідок втрати надійності систем. Це також важливо для адресної функціональності, що є підхарактеристикою надійності (див. ISO 9126). Наприклад, втрата надійності може призвести до:

- обману,
- втраченої частини ринку,
- демотивації штату,
- ненадійних постачальників,
- втрати довіри з боку клієнта,
- судової відповідальності, включаючи відповідальність за порушення законодавства про

захист даних.

Залежно від наданих відповідей на поставлені вище питання, має бути вирішено, чи будуть загальні збитки, що можуть виникнути внаслідок втрати надійності, значними, незначними чи нульовими. Це рішення має бути задокументовано.

## 10.2 Засоби конфіденційності

Типи загроз, що впливають на конфіденційність, наведено нижче разом з засобами захисту від цих загроз. Посилання на ці засоби, описано в розділі 8. Якщо це важливо для вибору засобів захисту, треба брати до уваги тип і характеристики інформаційної системи.

Потрібно відмітити, що більшість засобів захисту, наведених у підрозділі 8.1, надають «загальний» захист, тобто вони розраховані на ряд загроз та забезпечують захист через підтримування загального ефективного керування інформаційною безпекою. Тому вони не перераховані тут детально, але їх вплив не треба недооцінювати, і їх треба впроваджувати для загального ефективного захисту. Загрози наведено за абеткою.

### 10.2.1 Підслуховування

Один із шляхів отримання доступу до контрольованої інформації — це підслуховування, наприклад, записування інформації з лінії чи підслуховування телефонної розмови. Засоби захисту від цього наведено нижче.

1 Фізичні засоби. До них належать кімнати, стіни, будівлі тощо, що роблять підслуховування неможливим чи важким. Інший шлях зробити це — створити шуми. Цей тип захисту не викладений точно в розділі 8. У випадку використання телефонів, певний захист від підслуховування може забезпечити відповідне прокладення кабелю. Цей захист описано лише в ISO/IEC TR 13335-5.

2 Інформаційна політика безпеки. Інший шлях уникнути підслуховування — забезпечити суворі правила стосовно того, коли, де, та за яких умов треба обмінюватись контрольованою інформацією.

3 Захист конфіденційності даних. Ще один шлях захиститись від прослуховування — зашифровувати повідомлення перед відправленням. Докладніші відомості про це можна знайти в 8.2.5.

### 10.2.2 Електромагнітне випромінювання

Електромагнітне випромінювання може бути використане нападником, щоб отримати інформацію, яка обробляється інформаційною системою. Засоби захисту від електромагнітного випромінювання наведено нижче.

1 Фізичні засоби. Це може бути екранування кімнат, стін тощо, що не дозволить електромагнітному випромінюванню проходити через таке екранування; цей тип захисту не описаний докладно в 8.1.7 (це не є найдешевшим способом захисту від електромагнітного випромінювання).

2 Захист конфіденційності даних. Детально про цей вид захисту обговорення описано в 8.2.5. Треба відмітити, що цей захист застосовують тільки до тих пір, доки інформація зашифрована. Для інформації, яку обробляють, відображають чи друкують, цей захист не застосовують.

3. Використання комп'ютерного обладнання з низьким рівнем випромінювання. Знову ж таки, цей підхід не описано детально в розділі 8, але обладнання з вбудованим захистом може бути отримано.

### 10.2.3 Зловмисний код

Зловмисний код може призводити до втрати конфіденційності, наприклад, через перехоплення та розкриття паролів. Засоби захисту від нього приведено нижче.

1 Захист від зловмисного коду. Детальний опис захисту від зловмисного коду, описано в 8.2.3.

2 Реагування на порушення. Своєчасно надані звіти про будь-які незвичні порушення можуть зменшити збитки у разі ураження зловмисним кодом. Виявлені вторгнення можна використовувати для виявлення спроб отримати вхід до системи чи мережі. Детальніші відомості про це можна знайти в пункті 8.1.3.

### 10.2.4 Приховування ідентичності користувача

Приховування ідентичності користувача можна використовувати, щоб уникнути автентифікації, а також всіх служб та функцій безпеки, пов'язаних з нею. В результаті, кожного разу це може призводити до проблем конфіденційності, коли приховування уможливорює доступ до контрольованої інформації. Засоби захисту в цій сфері наведено нижче.

1 I&A. Приховування стає більш важким, коли застосовують засоби ідентифікації та автентифікації, що базуються на поєднанні чогось відомого, чогось наявного, а також внутрішніх характеристиках користувача (див. 8.2.1).

2 Контроль логічного доступу та аудит. Контроль логічного доступу не може відрізнити уповноваженого користувача від когось, хто видає себе за цього авторизованого користувача, але використання механізмів контролю доступу може звузити сферу впливу (див. 8.2.2). Переглядання та аналізування журналів аудиту може виявити несанкціоновані дії.

3 Захист від зловмисного коду. Оскільки один із шляхів отримання паролів — це введення зловмисного коду для їх перехоплення, має бути захист від таких програм.

4 Керування мережею. Ще один спосіб отримання контрольованого матеріалу — приховування користувача в потоці, наприклад, електронної пошти. Зараз ISO працює над декількома документами, що міститимуть подальшу інформацію про детальні засоби захисту мережної безпеки.

5 Захист конфіденційності даних. Якщо, з деяких причин, вищезгаданий тип захисту неможливий чи недостатній, можна впровадити додатковий захист під час шифрування важливих даних (див. 8.2.5).

#### **10.2.5 Неправильне направлення/перенаправлення повідомлень**

Неправильне направлення — це зловмисне чи незловмисне неправильне спрямування повідомлень, тоді як перенаправлення можна застосовувати як для добрих, так і для недобрих цілей. Перенаправлення може виконуватись, наприклад, для підтримання цілісності доступності. Неправильне направлення та перенаправлення повідомлень можуть призводити до втрати конфіденційності, якщо воно дозволяє несанкціонований доступ до цих повідомлень. Засоби захисту проти цього наведено нижче.

1 Керування мережею. Засоби захисту від неправильного направлення та перенаправлення можна знайти в інших документах ISO, що на сьогодні розробляються та містять подальшу інформацію про детальні засоби захисту мережної безпеки.

2 Захист конфіденційності даних. У випадках помилкового перенаправлення, щоб запобігти несанкціонованому доступу, повідомлення треба шифрувати. Докладніші відомості про це можна знайти в 8.2.5.

#### **10.2.6 Збої програмного забезпечення**

Збої програмного забезпечення можуть впливати на безпеку конфіденційності, якщо це програмне забезпечення захищає конфіденційність, наприклад програми контролю доступу чи шифрування, або ж якщо збої програмного забезпечення спричиняють зациклювання, наприклад, в операційній системі. Засоби захисту конфіденційності в цьому випадку наведено нижче.

1 Реагування на порушення. Кожен, хто помічає некоректну роботу програмного забезпечення, повинен звітувати про це відповідальній особі так швидко, як це можливо. Докладніші відомості може бути знайдено в 8.1.3.

2 Експлуатація. Деяких збоїв програмного забезпечення можна уникнути за допомогою тестування програм перед використанням та за допомогою контролю змін програмного забезпечення (див. 8.1.5).

#### **10.2.7 Крадіжки**

Крадіжки можуть піддавати небезпеці конфіденційність, якщо вкрадений компонент ІТ має будь-яку контрольовану інформацію, що може стати доступною крадію. Засоби захисту від крадіжок наведено нижче.

1 Фізичні засоби. Це може бути матеріальний захист, що робить доступ у будівлю, зону чи кімнату, яка містить комп'ютерне обладнання, складнішим, або це можуть бути специфічні засоби захисту від крадіжок (обидва види описано в 8.1.7).

2 Персонал. Засоби захисту персоналу (контролювання зовнішнього персоналу, угоди конфіденційності тощо) мають бути наявними для ускладнення крадіжок (див. 8.1.4).

3 Захист конфіденційності. Цей засіб захисту треба впроваджувати, якщо можлива крадіжка комп'ютерного обладнання, наприклад, портативних комп'ютерів, що містить контрольовану інформацію. Для докладніших відомостей дивіться 8.2.5.

4 Контроль носіїв інформації. Будь-який носій, що містить контрольований матеріал, треба захищати від крадіг (див. 8.1.5).

#### **10.2.8 Несанкціонований доступ до комп'ютерів, даних, служб та програм**

Несанкціонований доступ до комп'ютерів, даних, служб та програм може бути загрозою, якщо можливий доступ до будь-яких контрольованих матеріалів. Засоби захисту від несанкціонованого доступу охоплюють відповідну ідентифікацію та автентифікацію, контроль логічного доступу, аудит на рівні інформаційної системи та відокремлення мережі на мережному рівні.

1 І&А. Відповідні засоби ідентифікації та автентифікації використовувати в поєднанні з контролем логічного доступу для запобігання несанкціонованому доступу.

2 Контроль логічного доступу та аудит. Треба використовувати засоби захисту, описані в 8.2.2, для забезпечення контролю логічного доступу через використання механізмів контролю доступу. Переглядання та аналізування журналів аудиту може виявити несанкціоновану діяльність людей з правами доступу до системи

3 Відокремлення мережі. Для ускладнення несанкціонованого доступу треба зробити відокремлення мережі (див. 8.2.4).

4 Фізичний контроль доступу. Крім логічного контролю доступу, захист можна забезпечити фізичним контролем доступу (див. 8.1.7).

5 Контроль носіїв інформації. Якщо контрольовані дані зберігаються на інших носіях інформації (наприклад, дискетах), для захисту цих носіїв від несанкціонованого доступу потрібно застосовувати контроль носіїв інформації (8.1.5).

6 Захист конфіденційності даних. Якщо, з деяких причин, вищезазначений тип захисту неможливий чи недостатній, може бути забезпечений додатковий захист під час шифрування контрольованих даних, що зберігаються (див. 8.2.5).

### **10.2.9 Несанкціонований доступ до носіїв даних**

Несанкціонований доступ до носіїв даних, на яких зберігається якийсь конфіденційний матеріал, та їх використання можуть впливати на безпеку конфіденційності. Засоби захисту конфіденційності наведено нижче.

1 Експлуатація. Контроль носіїв можна застосовувати для забезпечення, наприклад, фізичного захисту, обліку носіїв інформації та гарантоване вилучення інформації, що зберігалася, щоб ніхто не міг отримати конфіденційний матеріал з попередньо очищеного носія (див. 8.1.5). Спеціальні заходи захисту треба вжити для переносних носіїв інформації, таких як дискети, магнітні стрічки та папір.

2 Фізичний захист. Відповідний захист кімнат (міцні стіни та вікна, а також фізичний контроль доступу) та аксесуари безпеки можуть захистити від несанкціонованого доступу (див. 8.1.7).

3 Захист конфіденційності даних. Додатковий захист контрольованої інформації на носіях даних може бути забезпечений за допомогою шифрування матеріалу. Необхідна добра система керування ключами для безпроблемного використання шифрування (див. 8.2.5).

### **10.3 Засоби контролю цілісності**

Типи загроз, що можуть впливати на безпеку цілісності, наведено нижче разом із засобами захисту від цих загроз. Наведені посилання на засоби, описано в розділі 8. Якщо це важливо для вибору засобів захисту, треба враховувати тип і характеристики інформаційної системи.

Потрібно відмітити, що більшість засобів захисту, наведених у підрозділі 8.1, забезпечують більш «загальний» захист, тобто вони націлені на певні загрози та забезпечують захист через підтримування загального ефективного керування інформаційною безпекою. Тому вони не описані тут детально, але їх вплив не треба недооцінювати, і їх треба впроваджувати для загального ефективного захисту. Загрози наведено за абетковою.

#### **Національна примітка.**

Упорядкування було здійснено згідно з англійським оригіналом ISO/IEC TR 13335-4:2002

### **10.3.1 Псування носіїв даних**

Псування носіїв даних загрожує цілісності інформації, що зберігається на цих носіях. Якщо цілісність є важливою, треба застосовувати такі засоби захисту.

1 Контроль носіїв інформації. Достатній контроль носіїв повинен охоплювати перевіряння цілісності (див. 8.1.5), щоб з'ясувати, що збережені файли були пошкоджені.

2 Резервування. Потрібно виконувати резервування всіх важливих файлів, ділових даних тощо. Якщо помічена втрата цілісності, наприклад, через контроль носіїв чи тестування резервних копій, тоді треба використати запасну копію чи попередню копію для відновлення цілісності файлів. Докладніші відомості про резервування можна знайти в 8.1.6.

3 Захист цілісності даних. Для захисту цілісності даних на запам'ятовувальному пристрої можуть бути впроваджені криптографічні методи. Докладніші відомості можна знайти в 8.2.5.

### **10.3.2 Помилки обслуговування**

Якщо обслуговування виконують нерегулярно чи під час обслуговування трапляються помилки, то цілісність інформації знаходиться під загрозою. Засоби захисту цілісності в цьому випадку наведено нижче.



1 Обслуговування. Належне обслуговування — це найкращий шлях уникнення помилок обслуговування (див. 8.1.5). Воно охоплює задокументовані та перевірені процедури обслуговування та належний нагляд за роботою.

2 Резервування. Якщо трапляються помилки обслуговування, для відновлення цілісності пошкодженої інформації можна використовувати резервні копії (див. 8.1.6).

3 Захист цілісності даних. Для захисту цілісності інформації можна використовувати криптографічні методи. Докладніші відомості можна знайти в 8.2.5.

### **10.3.3 Зловмисний код**

Зловмисний код може призвести до втрати цілісності, наприклад, якщо дані чи файли змінені особою, що отримала несанкціонований доступ з допомогою зловмисного коду чи самим цим кодом. Засоби захисту від цього наведено нижче.

1 Захист від зловмисного коду. Детальний опис захисту від зловмисного коду наведено у 8.2.3.

2 Реагування на порушення. Своєчасне звітування про будь-які незвичні порушення може зменшити збитки у разі ураження зловмисним кодом. Виявлення вторгнень треба використовувати для виявлення спроб виконати вхід до системи чи мережі. Докладнішу інформацію про це можна знайти в пункті 8.1.3.

### **10.3.4 Приховування ідентичності користувача**

Приховування ідентичності користувача можна використовувати для унеможливлення автентифікації, а також всіх служб та функцій безпеки, пов'язаних з нею. В результаті, воно може призводити до проблем конфіденційності кожний раз, коли це приховування унеможливлює доступ до інформації та її модифікацію. Засоби захисту в цій сфері наведено нижче.

1 I&A. Приховування стає більш важким, якщо застосовують засоби ідентифікації та автентифікації, які базуються на поєднанні чогось відомого, чогось наявного, а також внутрішніх характеристик користувача (див. 8.2.1).

2 Контроль логічного доступу та аудит. Контроль логічного доступу не може відрізнити уповноваженого користувача від того, хто видає себе за цього уповноваженого користувача, але використання механізмів контролю доступу може зменшити сферу впливу (див. 8.2.2). Переглядання та аналізування журналів аудиту можуть виявити несанкціоновані дії.

3 Захист від зловмисного коду. Оскільки один із способів отримання паролів — це введення зловмисного коду для їх перехоплення, то має бути захист від таких програм.

4 Керування мережею. Ще один спосіб несанкціонованого доступу — приховування користувача в потоці, наприклад, електронної пошти. Зараз ISO працює над декількома документами, що міститимуть подальшу інформацію про детальні засоби захисту мережної безпеки.

5 Захист цілісності даних. Якщо, з деяких причин, вищезгаданий тип захисту неможливий чи недостатній, треба забезпечити додатковий захист у разі використання криптографічних методів, таких як цифрові підписи (див. 8.2.5).

### **10.3.5 Неправильне направлення/перенаправлення повідомлень**

Неправильне направлення — це зловмисне чи незловмисне хибне спрямування повідомлень, тоді як перенаправлення можна застосовувати як для добрих, так і для недобрих цілей. Перенаправлення може виконуватись, наприклад, для підтримування цілісності доступності. Неправильне направлення та перенаправлення повідомлень може призводити до втрати цілісності, наприклад, якщо повідомлення були змінені, а потім надіслані до первісного адресата. Засоби захисту проти цього наведено нижче.

1 Керування мережею. Засоби захисту від неправильного направлення та перенаправлення можна знайти в інших документах ISO, що в теперішній час розробляються та містять наступну інформацію про детальні засоби захисту мережної безпеки.

2 Захист цілісності даних. Для запобігання несанкціонованій зміні доступу у випадках помилкового направлення та перенаправлення, можна використовувати геш-функції та цифрові підписи. Докладнішу інформацію про це можна знайти в 8.2.5.

### **10.3.6 Неспростовність**

Засоби для забезпечення неспростовності треба застосовувати, коли важливо мати підтвердження того, що повідомлення було відправлено та (або) отримано, і що мережа передала це повідомлення. Існують специфічні криптографічні засоби захисту як основа неспростовності, що описані в пункті 8.2.5 (цілісність даних та неспростовність).

### 10.3.7 Збої програмного забезпечення

Збої програмного забезпечення можуть зруйнувати цілісність даних та інформації, яку обробляють за допомогою цього програмного забезпечення. Засоби захисту цілісності наведено нижче.

1 Звітування про некоректне функціонування програмного забезпечення. Звітування про збої, проведене швидко, наскільки це можливо, допомагає зменшити збитки, якщо такі збої виникають (див. 8.1.3).

2 Експлуатація. Контроль за безпекою можна використовувати для гарантування того, що програмне забезпечення функціонує коректно та контроль змін програмного забезпечення може уникнути проблем через оновлення чи внесення змін до програмного забезпечення.

3 Резервування. Резервні копії, наприклад, створені раніше, можна використовувати для відновлення цілісності даних, що були оброблені програмним забезпеченням, яке не функціонує коректно (див. 8.1.6).

4 Захист цілісності даних. Для захисту цілісності даних можна використовувати криптографічні методи. Докладнішу інформацію можна знайти в 8.2.5.

### 10.3.8 Збої постачання (живлення, кондиціонування повітря)

Збої постачання можуть викликати проблеми цілісності, якщо через них виникли інші збої. Наприклад, збої постачання можуть спричинити збої апаратного забезпечення, технічні пошкодження чи проблеми з накопичувачами інформації. Засоби захисту від цих специфічних проблем можна знайти у відповідних підпунктах; засоби захисту від збоїв постачання наведено нижче.

1 Живлення та кондиціонування повітря. Треба використовувати засоби захисту живлення та кондиціонування повітря, наприклад, захист від сплесків напруги, коли необхідно уникнути будь-яких проблем, пов'язаних зі збоями постачання (див. 8.1.7).

2 Резервування. Резервування треба використовувати для відновлення пошкодженої інформації (див. 8.1.6).

### 10.3.9 Технічні пошкодження

Технічні пошкодження, наприклад, у мережі, можуть зруйнувати цілісність будь-якої інформації, що зберігається чи обробляється в цій мережі. Засоби захисту від технічних пошкоджень наведено нижче.

1 Експлуатація. Керування конфігурацією та змінами, так само, як керування потужностями, треба використовувати, щоб уникнути збоїв у будь-якій системі чи мережі. Документацію та обслуговування використовують для забезпечення безперебійної роботи системи чи мережі (див. 8.1.5).

2 Керування мережею. Для мінімізації ризиків технічних пошкоджень треба використовувати методику експлуатації, планування системи та належну конфігурацію мережі (див. 8.2.4).

3 Електричне живлення та кондиціонування повітря. Треба використовувати засоби захисту живлення та кондиціонування повітря, наприклад, захист від коливань напруги, коли необхідно уникнути будь-яких проблем, пов'язаних зі збоями постачання (див. 8.1.7).

4 Резервування. Резервування треба використовувати для відновлення пошкодженої інформації (див. 8.1.6).

### 10.3.10 Помилки передавання

Помилки передавання можуть зруйнувати цілісність інформації, що передається. Засоби захисту цілісності наведено нижче.

1 Прокладання кабелю. Ретельне планування та прокладання кабелю допоможуть уникнути помилок, наприклад, якщо помилка спричинена перевантаженням (див. також 8.1.7).

2 Керування мережею. Мережним обладнанням треба належним чином керувати та обслуговувати його, щоб уникнути помилок передавання. Зараз ISO працює над декількома документами, що містять наступну інформацію про детальні засоби захисту мережної безпеки, які можна буде використати для захисту від помилок передавання.

3 Захист цілісності даних. Для захисту від випадкових помилок передавання в протоколах передавання даних можна використовувати контрольні суми та циклічні надлишкові коди (CRC). Для захисту цілісності даних від зловмисних атак під час передавання використовують криптографічні методи. Докладнішу інформацію можна знайти в 8.2.5.

### **10.3.11 Несанкціонований доступ до комп'ютерів, даних, служб та програм**

Несанкціонований доступ до комп'ютерів, даних, служб та програм може бути загрозою цілісності інформації, якщо можлива несанкціонована модифікація. Засоби захисту від несанкціонованого доступу охоплюють належну ідентифікацію та автентифікацію, контроль логічного доступу, аудит на рівні інформаційної системи, та поділ мережі на мережному рівні.

1 I&A. Для запобігання несанкціонованому доступу відповідні засоби ідентифікації та автентифікації треба використовувати разом з контролем логічного доступу.

2 Контроль логічного доступу та аудит. Треба використовувати засоби захисту, описані в 8.2.2, для забезпечення контролю логічного доступу через використання механізмів контролю доступу. Переглядання та аналізування журналів аудиту може виявити недозволені дії працівників, що су-перечать правам доступу до системи.

3 Поділ мережі. Для ускладнення несанкціонованого доступу треба зробити поділ мережі (див. 8.2.4).

4 Фізичний контроль доступу. Крім логічного контролю доступу, захист може забезпечуватись фізичним контролем доступу (див. 8.1.7).

5 Контроль носіїв інформації. Якщо контрольовані дані зберігаються на інших носіях інфор-мації (наприклад, дискетах), для захисту цих носіїв від несанкціонованого доступу треба засто-сувати контроль носіїв інформації (8.1.5).

6 Цілісність даних. Для захисту цілісності даних під час зберігання чи передавання викорис-товують криптографічні методи. Докладнішу інформацію можна знайти в 8.2.5.

### **10.3.12 Використання несанкціонованих програм та даних**

Використання несанкціонованих програм та даних піддає небезпеці цілісність інформації, яка зберігається та обробляється з системою, якщо програми та дані використовуються для зміни інформації несанкціонованим шляхом, або якщо програми та дані містять зловмисний код (наприк-лад ігри). Засоби захисту від цього наведено нижче.

1 Інформування про безпеку та навчання. Всі працівники мають бути попереджені про те, що вони не повинні інсталиувати та використовувати жодне програмне забезпечення без дозволу ке-рівника інформаційної безпеки або будь-кого, хто може відповідати за безпеку системи (див. та-кож 8.1.4).

2 Резервування. Резервування треба використовувати для відновлення пошкодженої інфор-мації (див. 8.1.6).

3 I&A. Відповідні засоби ідентифікації та автентифікації треба використовувати разом з кон-тролем логічного доступу для запобігання несанкціонованому доступу.

4 Контроль логічного доступу та аудит. Контроль логічного доступу, описаний в 8.2.2, має га-рантувати, що тільки уповноважені особи можуть застосовувати програмне забезпечення для об-роблення та зміни інформації. Переглядання та аналізування журналів аудиту може виявити не-санкціоновані дії.

5 Захист від зловмисного коду. Перед використанням всі програми та дані треба перевіряти на наявність зловмисного коду (див. 8.2.3).

### **10.3.13 Несанкціонований доступ до носіїв даних**

Несанкціонований доступ та використання носія даних може піддавати небезпеці цілісність, оскільки він дозволяє несанкціоновану зміну інформації, що зберігається на цьому носії. Засоби захисту цілісності наведено нижче.

1 Експлуатація. Контроль носіїв можна застосовувати для забезпечення, наприклад, фізичного захисту, ідентифікованості носіїв інформації, для запобігання несанкціонованому доступу, а пере-віряння цілісності — для виявлення будь-якого порушення цілісності інформації на носії (див. 8.1.5). Спеціальні заходи запровадити для захисту легкозмінних носіїв інформації, таких як дис-кети, магнітні стрічки та папір.

2 Фізичний захист. Відповідний захист кімнат (міцні стіни та вікна, а також максимально мож-ливий контроль фізичного доступу) та аксесуари безпеки можуть захистити від несанкціоновано-го доступу (див. 8.1.7).

3 Цілісність даних. Для захисту цілісності даних під час їхнього зберігання на носії інформації використовують криптографічні методи. Докладнішу інформацію можна знайти в 8.2.5.

### 10.3.14 Помилки користувача

Помилки користувача можуть зруйнувати цілісність інформації. Засоби захисту від них наведено нижче.

1 Інформування про безпеку та навчання. Всі користувачі мають бути навчені належним чином, щоб уникнути помилок під час оброблення інформації (див. також 8.1.4). Це навчання має охоплювати тренування на визначення дій процедури експлуатації чи безпеки.

2 Резервування. Резервні копії, наприклад, створені раніше, можна використовувати для відновлення цілісності даних, які було знищено через помилки користувача (див. 8.1.6).

### 10.4 Засоби захисту доступності

Типи загроз, що можуть піддавати небезпеці доступність, наведено нижче разом із засобами захисту від цих загроз. Наведені посилання на засоби, описані в розділі 8. Якщо це важливо для вибору засобів захисту, треба враховувати до уваги тип і характеристики інформаційної системи.

Потрібно відмітити, що більшість засобів захисту, наведених у підрозділі 8.1, забезпечують "загальний" захист, тобто вони не націлені на окремі загрози, а забезпечують захист через підтримання загального ефективного керування інформаційною безпекою. Тому вони не описані тут детально, але їх вплив не треба недооцінювати, і вони мають бути реалізовані для загального ефективного захисту.

Вимоги до доступності можуть коливатися від некритичних за часом даних або ІТ систем (але втрата таких даних та непрацездатність таких систем все ще вважається критичною) до надто критичних за часом даних або систем. Перші треба захищати резервуванням, в той час як останні можуть потребувати наявності резервної системи. Типи загроз впорядковано за абеткою.

#### Національна примітка

Упорядкування за абеткою виконано для англійського оригіналу ISO/IEC TR 13335-4:2002.

#### 10.4.1 Руйнівний напад

Інформація може бути знищена під дією руйнівних нападів. Засоби захисту проти них наведено нижче.

1 Дисциплінарний процес. Всі працівники мають бути попереджені про наслідки у випадку, якщо вони (зловмисно чи незловмисно) знищують інформацію (див. також 8.1.4).

2 Контролювання носіїв інформації. Всі носії інформації мають бути відповідно захищеними від несанкціонованого доступу, використовуючи фізичний захист та облік всіх носіїв (див. 8.1.5).

3 Резервування. Треба робити резервні копії всіх важливих файлів, ділових даних тощо. Якщо файл чи будь-яка інша інформація недоступна (з будь-якої причини), для відновлення інформації треба використовувати резервну копію чи попередню резервну копію. Докладніше про резервування можна знайти в 8.1.6.

4 Матеріальний захист. Для запобігання несанкціонованому доступу, що сприятиме несанкціонованому руйнуванню комп'ютерного обладнання чи інформації (див. 8.1.7), треба використовувати фізичний контроль за доступом.

5 I&A. Відповідні засоби ідентифікації та автентифікації треба використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу.

6 Контролювання та аудит логічного доступу. Контролювання логічного доступу, описане в 8.2.2, повинно гарантувати, що не буде несанкціонованого доступу до інформації, який може її знищити. Переглядання та аналізування журналів аудиту може виявити несанкціоновані дії.

#### 10.4.2 Псування носіїв даних

Псування носіїв даних загрожує доступності інформації, що зберігається на цих носіях. Якщо доступність є важливим чинником, треба застосовувати такі засоби захисту.

1. Контролювання носіїв інформації: Регулярне тестування носіїв даних має виявляти будь-яке псування, бажано до того, як інформація стане дійсно недоступною. Носії мають зберігатись у такий спосіб, щоб не було ніякого зовнішнього впливу, який міг би спричинити псування (див. 8.1.5).

2 Резервування. Треба робити резервні копії всіх важливих файлів, ділових даних тощо. Якщо файл чи будь-яка інша інформація недоступна (з будь-якої причини), для відновлення інформації треба використовувати резервну копію чи попередню резервну копію. Детальніше про резервування можна знайти в 8.1.6.

#### **10.4.3 Збої комунікаційного обладнання та служб**

Збої комунікаційного обладнання та служб загрожують доступності інформації, що передається за допомогою цих послуг. Залежно від причин збою, може бути корисним розглянути положення у 10.4.11 «Збої програмного забезпечення», 10.4.12 «Збої постачання» чи 10.4.13 «Технічні несправності». Засоби захисту доступності наведено нижче.

1 Надлишковість та резервування. Надмірне запровадження компонентів комунікаційних служб може бути використано для зниження ймовірності збоїв комунікаційних служб. Залежно від розміру максимального припустимого простою, запасне обладнання також можна використовувати для задоволення потреб. У будь-якому випадку, дані конфігурації та розташування мають бути також зарезервовані для забезпечення доступності у випадку надзвичайної ситуації. Загальна інформація про резервування може бути знайдена в 8.1.6.

2 Керування мережею. Зараз ISO працює над декількома документами, що містять подальшу інформацію про детальні засоби захисту мережної безпеки, яка може бути застосована для захисту від збоїв комунікаційного обладнання чи служб.

3 Прокладання кабелю. Ретельне планування та прокладання кабелю можуть запобігти пошкодженням; якщо є підозра, що лінію може бути пошкоджено, цю версію потрібно перевірити (див. також 8.1.7).

4 Неспростовність. Якщо потребують підтвердження мережного доставлення, посилання чи отримання повідомлення, треба застосовувати неспростовність (див. 8.2.5); тоді пошкодження комунікацій чи зниклу інформацію можна легко виявити.

#### **10.4.4 Вогонь, вода**

Інформація та комп'ютерне обладнання можуть бути знищені вогнем та (або) водою. Засоби захисту від вогню та води наведено нижче.

1 Фізичний захист. Всі будівлі та кімнати, які містять комп'ютерне обладнання чи носії, що зберігають важливу інформацію, треба належним чином захищати від вогню і води (див. 8.1.7).

2 План неперервності бізнесу. Для захисту бізнесу від згубних впливів вогню та води треба розробити план неперервності бізнесу та доступні резервні копії важливої інформації (див. 8.1.6).

#### **10.4.5 Помилки обслуговування**

Якщо обслуговування виконують нерегулярно чи в процесі його виконання трапляються помилки, то доступність інформації знаходиться під загрозою. Засоби захисту в цьому випадку наведено нижче.

1 Обслуговування. Належне обслуговування — це найкращий шлях уникнути помилок обслуговування (див. 8.1.5).

2 Резервування. Якщо трапляються помилки обслуговування, для відновлення доступності втраченої інформації можна використовувати резервні копії (див. 8.1.6).

#### **10.4.6 Зловмисний код**

Зловмисний код можна використовувати, щоб обійти автентифікацію та всі служби і функції безпеки, пов'язані з нею. Унаслідок цього, він може призвести до втрати доступності, наприклад, якщо дані чи файли знищені особою, яка отримала несанкціонований доступ з допомогою зловмисного коду, чи безпосередньо зловмисним кодом.

Засоби захисту проти нього наведено нижче.

1 Захист від зловмисного коду. Детальний опис захисту від зловмисного коду дивіться у 8.2.3.

2 Реагування на порушення. Своєчасне звітування про будь-які незвичні порушення може обмежити пошкодження від ураження зловмисним кодом. Виявлення вторгнень можна використовувати, щоб виявити спроби входу до системи чи мережі. Детальнішу інформацію про це можна знайти у пункті 8.1.3.

#### **10.4.7 Приховування особистості користувача**

Приховування особистості користувача можна використовувати, щоб обійти автентифікацію, а також усі служби та функції безпеки, пов'язані з нею. В результаті, воно може призводити до проблем доступності кожного разу, коли це приховування дозволяє вилучити або знищити інформацію. Засоби захисту в цій сфері наведено нижче.

1 I&A. Приховування стає важчим, якщо застосовують засоби ідентифікації та автентифікації, які базуються на комбінаціях чогось відомого, чогось наявного, а також внутрішніх характеристиках користувача (див. 8.2.1).

2 Контроль та аудит логічного доступу. Контроль логічного доступу не може відрізняти авторизованого користувача від когось, хто видає себе за цього авторизованого користувача, але використання механізмів контролю доступу може зменшити сферу впливу (див. 8.2.2). Переглядання та аналізування журналів аудиту може виявити несанкціоновані дії.

3 Захист від зловмисного коду. Оскільки один із шляхів отримання паролів — це введення зловмисного коду для їх перехоплення, має бути захист від таких програм.

4 Керування мережею. Ще один спосіб неуповноваженого доступу — приховування користувача в потоці, наприклад, електронної пошти. Зараз ISO працює над декількома документами, що містять подальшу інформацію про детальні засоби захисту мережної безпеки.

5 Резервування даних. Резервування даних не може захистити від приховування особистості користувача, але зменшує вплив подій, пов'язаних з пошкодженням, що виникають внаслідок цього (див. 8.1.6).

#### **10.4.8 Неправильне направлення/перенаправлення повідомлень**

Неправильне направлення — це зловмисне чи незловмисне неправильне спрямування повідомлень, у той час, як перенаправлення можна застосовувати як для добрих, так і для недобрих цілей. Перенаправлення можна виконувати, наприклад, для підтримування цілісності доступності. Неправильне направлення та перенаправлення повідомлень призводять до втрати доступності повідомлень. Засоби захисту проти цього наведено нижче.

1 Керування мережею. Засоби захисту від неправильного направлення та перенаправлення можна знайти в інших документах ISO, що на теперішній час перебувають на етапі розроблення і містять подальшу інформацію про детальні засоби захисту мережної безпеки.

2 Неспровствність. Якщо є потреба підтвердити мережне доставлення, відправлення або отримання повідомлення, треба застосовувати неспровствність (див. 8.2.5).

#### **10.4.9 Зловживання ресурсами**

Зловживання ресурсами може призвести до недоступності інформації чи служб. Засоби захисту від цього наведено нижче.

1 Персонал. Весь персонал має бути попереджений про наслідки зловживання ресурсами; за потреби треба запровадити дисциплінарні заходи (див. 8.1.4).

2 Експлуатація. Для виявлення несанкціонованих дій за системою потрібно слідкувати, а для мінімізації можливостей зловживання привілеями треба провадити розподіл обов'язків (див. 8.1.5).

3 I&A. Відповідні засоби ідентифікації та автентифікації треба використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу.

4 Контроль та аудит логічного доступу. Треба використовувати засоби захисту, описані в 8.2.2, для забезпечення контролю логічного доступу через використання механізмів контролю доступу. Переглядання та аналізування журналів аудиту може виявити несанкціоновані дії.

5 Керування мережею. Для мінімізації можливостей зловживання ресурсами в мережах треба застосовувати відповідну конфігурацію та розподіл мережі (див. 8.2.4).

#### **10.4.10 Стихійні лиха**

Для захисту від втрати інформації та послуг через стихійні лиха треба застосовувати такі засоби захисту.

1 Захист від стихійних лих. Всі будівлі мають бути захищені, наскільки це можливо, від стихійних лих (див. 8.1.7).

2 План неперервності бізнесу. Має бути наявний та повністю перевірений план неперервності бізнесу для кожної будівлі, резервних копій всієї важливої інформації, мають бути доступні служби та ресурси (див. 8.1.6).

#### **10.4.11 Збої програмного забезпечення**

Збої програмного забезпечення можуть знищити доступність даних та інформацію, що обробляється цим програмним забезпеченням. Засоби захисту доступності наведено нижче.

1 Звітування про збої програмного забезпечення. Звітування про збої якомога швидше, допоможе обмежити пошкодження у випадку їх виникнення (див. 8.1.3).

2 Експлуатація. Тестування безпеки можна використовувати для гарантування коректного функціонування програмного забезпечення, а контроль змін програмного забезпечення допоможе уникнути проблем цих програм, спричинених оновленнями чи іншими змінами програмного забезпечення (див. 8.1.5).

3 Резервування. Резервні копії, наприклад, зроблені останніми, можна використовувати для відновлення даних, оброблених програмним забезпеченням, що функціонує некоректно (див. 8.1.6).

#### **10.4.12 Збої постачання (живлення, кондиціонування повітря)**

Збої постачання можуть викликати проблеми доступності, якщо через них виникли інші збої. Наприклад, пошкодження постачання можуть спричинити збої апаратного забезпечення, технічні пошкодження чи проблеми з накопичувачами інформації. Засоби захисту від цих специфічних проблем можна знайти у відповідних підпунктах; засоби захисту від збоїв постачання наведено нижче.

1 Живлення та кондиціонування повітря. Треба використовувати засоби захисту живлення та кондиціонування повітря, наприклад, захист від сплесків напруги, коли необхідно уникнути будь-яких проблем, пов'язаних зі збоями постачання (див. 8.1.7).

2 Резервування. Треба робити резервні копії всіх важливих файлів, ділових даних тощо. Якщо файл чи будь-яка інша інформація втрачена через збої постачання, для відновлення інформації треба використовувати резервну копію чи попередню резервну копію. Докладніше про резервування можна знайти в 8.1.6.

#### **10.4.13 Технічні пошкодження**

Технічні пошкодження, наприклад, у мережах, можуть знищити доступність будь-якої інформації, що зберігається чи обробляється в цій мережі. Засоби захисту від технічних пошкоджень наведено нижче.

1 Експлуатація. Керування конфігурацією та змінами, так само, як і керування потужностями, треба використовувати, щоб уникнути збоїв будь-якої ІТ системи. Документацію та обслуговування використовують для забезпечення безпроблемної роботи системи (докладніше про це в 8.1.5).

2 Керування мережею. Для мінімізації ризиків технічних пошкоджень треба використовувати методику експлуатації, планування системи та відповідну конфігурацію мережі (див. 8.2.4).

3 План неперервності бізнесу. Для захисту бізнесу від пагубних ефектів технічних пошкоджень, треба розробити план неперервності бізнесу та доступні резервні послуги, ресурси та копії важливої інформації (див. 8.1.6).

#### **10.4.14 Крадіжки**

Крадіжки явно піддають небезпеці доступність інформації та ІТ обладнання. Засоби захисту від крадіжок наведено нижче.

1 Фізичні засоби. Це може бути матеріальний захист, що робить доступ в будівлю, зону чи кімнату, яка містить комп'ютерне обладнання та інформацію, складнішим, або це можуть бути специфічні засоби від крадіжок (обидва види описані в 8.1.7).

2 Персонал. Для ускладнення крадіжок мають бути наявні засоби захисту персоналу (контролювання зовнішнього персоналу, угоди конфіденційності тощо) (див. 8.1.4).

3 Контроль носіїв інформації. Будь-який носій, що містить важливий матеріал, треба захищати від крадіжок (див. 8.1.5).

#### **10.4.15 Перевантаження каналів**

Перевантаження каналів загрожує доступності інформації, що передається по цих каналах. Засоби захисту доступності наведено нижче.

1 Надлишковість та резервування. Надлишкова реалізація компонентів комунікаційних послуг може бути використана для зниження ймовірності збоїв комунікаційних служб. Залежно від розміру максимального припустимого простою, запасне обладнання також треба використовувати для задоволення вимог. У будь-якому випадку, дані конфігурації та розташування мають бути також зарезервовані для забезпечення доступності у випадку надзвичайної ситуації. Загальну інформацію про резервування можна знайти в 8.1.6.

2 Керування мережею. Щоб уникнути перевантаження треба використовувати відповідну конфігурацію, керування і адміністрування мереж та комунікаційних послуг.

3 Керування мережею. Зараз ISO розробляє документи, що містять подальшу інформацію про детальні засоби захисту мережної безпеки, яка може бути застосована для захисту від перевантаження каналів.

#### **10.4.16 Помилки передавання**

Помилки передавання можуть зруйнувати доступність інформації, що передається. Засоби захисту доступності наведено нижче.

1 Прокладання кабелю. Ретельне планування та прокладання кабелю можуть допомогти уникнути помилок передавання, наприклад, якщо помилка викликана перевантаженням (див. також 8.1.7).

2 Керування мережею. Керування мережею не може захистити від помилок передавання, а може використовуватись для виявлення проблем, що виникають через помилки передавання та підняття тривоги в таких випадках. Це дозволяє своєчасно реагувати на такі проблеми. Зараз ISO розробляє документи, що містять подальшу інформацію про детальні засоби захисту мережної безпеки, яка може бути застосована для захисту від помилок передавання.

#### **10.4.17 Несанкціонований доступ до комп'ютерів, даних, служб та програм**

Несанкціонований доступ до комп'ютерів, даних, служб та програм може бути загрозою доступності інформації, якщо можливий несанкціонований доступ. Засоби захисту від несанкціонованого доступу охоплюють відповідну ідентифікацію та автентифікацію, контроль логічного доступу, аудит на рівні інформаційної системи та поділ мережі на мережному рівні.

1 I&A. Відповідні засоби ідентифікації та автентифікації треба використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу.

2 Контроль та аудит логічного доступу. Треба використовувати засоби захисту, описані в 8.2.2, для забезпечення контролю логічного доступу через використання механізмів контролю доступу. Переглядання та аналізування журналів аудиту може виявити неуповноважені дії співробітників з правами доступу до системи.

3 Поділ мережі. Щоб несанкціонований доступ до мережі був важчим, треба здійснити поділ мережі (див. 8.2.4).

4 Контроль фізичного доступу. Крім логічного контролю доступу, захист можна забезпечувати фізичним контролем доступу (див. 8.1.7).

5 Контроль носіїв інформації. Якщо важливі дані зберігаються на інших носіях інформації (наприклад, дискетах), для захисту цих носіїв від несанкціонованого доступу потрібно застосовувати контроль носіїв інформації (8.1.5).

#### **10.4.18 Використання несанкціонованих програм та даних**

Використання несанкціонованих програм та даних піддає небезпеці доступність інформації, що зберігається та обробляється в системі, в якій це відбувається, якщо програми та дані використовують для вилучення інформації несанкціонованим шляхом, або якщо програми та дані містять зловмисний код (наприклад, ігри). Засоби захисту від цього наведено нижче.

1 Інформування про безпеку та навчання. Всі працівники мають бути попереджені про те, що вони не повинні запускати жодне програмне забезпечення без дозволу керівника інформаційної безпеки або будь-кого, хто може відповідати за безпеку системи (див. також 8.1.4).

2 Резервування. Резервні копії треба використовувати для відновлення пошкодженої інформації (див. 8.1.6).

3 I&A. Відповідні засоби ідентифікації та автентифікації треба використовувати разом з контролем логічного доступу для запобігання несанкціонованому доступу.

4 Контроль та аудит логічного доступу. Контроль логічного доступу, описаний в 8.2.2, повинен гарантувати, що тільки уповноважені особи можуть застосовувати програмне забезпечення для оброблення та вилучення інформації. Переглядання та аналізування журналів аудиту може виявити несанкціоновані дії.

5 Захист від зловмисного коду. Перед використанням всі програми та дані треба перевіряти на наявність зловмисного коду (див. 8.2.3).

#### **10.4.19 Несанкціонований доступ до носіїв даних**

Несанкціонований доступ та використання носія даних може піддавати небезпеці доступність, оскільки він може спричинити несанкціоноване знищення інформації, яка зберігається на цьому носії. Засоби захисту конфіденційності наведено нижче.

1 Експлуатація. Контроль носіїв можна застосовувати для забезпечення, наприклад, фізичного захисту, обліку носіїв інформації для запобігання несанкціонованому доступу до інформації, що зберігають на цих носіях (див. 8.1.5). Спеціальні заходи треба вжити для захисту легко змінних носіїв інформації: дискети, магнітні стрічки та папір.

2 Фізичний захист. Відповідний захист кімнат (міцні стіни та вікна, а також контроль фізичного доступу) та аксесуари безпеки захищають від несанкціонованого доступу (див. 8.1.7).



#### **10.4.20 Помилки користувача**

Помилки користувача можуть знижити доступність інформації. Засоби захисту від них наведено нижче.

1 Інформування про безпеку та навчання. Всі користувачі мають бути відповідно навчені, щоб уникнути помилок під час оброблення інформації (див. також 8.1.4). Це навчання повинно охоплювати тренування, яке навчає визначеним таким діям, як процедури експлуатації чи безпеки.

2 Резервування. Резервні копії, наприклад, створені попереднього разу, можна використовувати для відновлення інформації, що була знищена через помилки користувача (див. 8.1.6).

#### **10.5 Засоби захисту спостережності, автентичності та надійності**

Сфера застосування спостережності, автентичності та надійності дуже відрізняється в різних галузях. Ці відмінності означають, що можна застосувати багато різних засобів захисту. Тому нижче наведено загальну настанову.

Засоби захисту, наведені у підрозділі 8.1, забезпечують «загальний» захист, тобто вони спрямовані на низку загроз та забезпечують захист через підтримання загального ефективного керування інформаційною безпекою. Тому вони не наведені тут, але їх вплив не треба недооцінювати, і їх треба впроваджувати для загального ефективного захисту.

##### **10.5.1 Спостережність**

Для захисту спостережності можна розглядати будь-яку загрозу, що може призвести до неможливості пов'язати якісь дії з конкретним об'єктом чи суб'єктом. Деякі приклади таких загроз: спільне використання облікового запису, відсутність трасування дій, приховування особистості користувача, збої програмного забезпечення, несанкціонований доступ до комп'ютерів, даних, служб та програм, а також слабка автентифікація особистості.

Є два типи спостережності, які необхідно розглянути. Один пов'язаний з визначенням користувачів, відповідальних за конкретні дії над інформацією та інформаційними системами. Цю функцію виконують журнали аудиту. Інший тип пов'язаний з ідентифікованістю між користувачами в системі. Його можна досягнути через послуги неспростовності, розділення знань та подвійний контроль.

Багато засобів захисту можна використовувати для впровадження неспростовності чи сприяти її запровадженню. Можна застосовувати засоби, що залежать від таких чинників: політика безпеки, інформування про безпеку та контроль і аудит логічного доступу до одноразових паролів та контролю носіїв інформації. Впровадження політики володіння інформацією є необхідною умовою спостережності. Вибір специфічних засобів захисту буде залежати від визначеного використання спостережності в конкретній сфері.

##### **10.5.2 Автентичність**

Може бути зменшена будь-яка загроза, яка може призводити до того, що суб'єкт, система чи процес не будуть упевнені в автентичності об'єкта. Наприклад, ситуації, що можуть призвести до виникнення цього, містять неконтрольовані зміни даних, неперевірене джерело даних та джерело даних, що не підтримується.

Багато засобів захисту можна використовувати для впровадження автентичності чи сприяти її впровадженню. Можна застосовувати засоби від підписаних довідкових даних, контролю та аудиту логічного доступу до використання цифрових підписів. Вибір специфічних засобів захисту буде залежати від визначеного використання автентичності в конкретній сфері.

##### **10.5.3 Надійність**

Будь-яка загроза, що може призвести до суперечливої поведінки систем чи процесів, зменшить рівень надійності. До таких загроз належать продуктивність системи та ненадійне обслуговування. Втрата надійності може проявитися в неякісній роботі з клієнтами чи втраті довіри клієнтів.

Багато засобів захисту можна використовувати для впровадження надійності чи сприяти її впровадженню. Можна застосовувати такі засоби, як плани неперервності бізнесу, введення надлишковості у фізичну архітектуру та обслуговування системи до ідентифікації і автентифікації, контролю і аудиту логічного доступу. Вибір специфічних засобів захисту буде залежати від визначеного використання автентичності в конкретній сфері.

## 11 ВИБІР ЗАСОБІВ ЗАХИСТУ ВІДПОВІДНО ДО ДЕТАЛЬНИХ ОЦІНОК

Вибір засобів захисту відповідно до детальних оцінок здійснюють згідно з принципами, наведеними в попередніх розділах. Детальне аналізування ризиків дозволяє враховувати спеціальні вимоги та обставини інформаційної системи та її цінностей. Відмінність від використання, наведеного у попередніх розділах — це обсяг робіт та подробиці, зібрані протягом процесу оцінювання. Тому можливе кваліфіковане обґрунтування вибраних засобів захисту. У пункті 11.1 зазначено, як ISO/IEC TR 13335-3, що описує метод аналізування ризиків, може бути використаний у процесі вибору засобів захисту, наведених у цій частині ISO/IEC TR 13335. Принципи вибору описано в 11.2.

### 11.1 Взаємозв'язок ISO/IEC TR 13335-3 та ISO/IEC TR 13335-4

В ISO/IEC TR 13335-3 описано керування інформаційною безпекою. Крім того, наведено інші питання, можливі варіанти корпоративної стратегії аналізування ризиків та рекомендований підхід до аналізування ризиків. Головними варіантами стратегій для використання в організації є:

- використання базового підходу для всіх ІТ систем,
- використання детального аналізування ризиків для всіх ІТ систем та
- використання «рекомендованого підходу», тобто дотримуватися високорівневого аналізування ризиків для всіх ІТ систем, базового підходу для ІТ систем малого ризику і детального аналізування ризиків для ІТ систем високого ризику.

Якщо для визначення засобів захисту було вирішено використовувати детальне аналізування ризиків для всіх ІТ систем, інформація про те, як вибирати засоби захисту, і як ефективно використовувати результати детального аналізування ризиків, наведено в пункті 11.2 цієї частини ISO/IEC TR 13335. Проте може використовуватися інформація про засоби захисту для специфічних ІТ систем та зв'язок між проблемами безпеки, загрозами і засобами захисту, які містяться в розділах 8—10 цієї частини ISO/IEC TR 13335.

### 11.2 Принципи вибору

Є чотири основних аспекти, на які спрямований засіб захисту: впливи, загрози, вразливості та ризики самі по собі. Засоби спрямовують на самі ризики, коли приймається рішення зменшити чи уникнути ризиків, а не приймати їх, наприклад, для зменшення ризику — проведення страхування, а прикладом, щоб уникнути ризику, є переміщення контрольованої інформації на інший комп'ютер. Компоненти, що всі разом створюють ризики, тобто впливи, загрози та вразливості, є головними цілями засобів захисту. Способи, якими засоби можна направляти на ці аспекти, такі:

1) загрози — засоби захисту можуть зменшити ймовірність виникнення загрози (наприклад, розглянемо загрозу втрати даних через помилки користувача, тоді навчальний курс для користувачів зменшить кількість цих помилок), чи, у випадку зловмисного нападу, вони можуть спинити його через збільшення технічної складності успішної атаки;

2) вразливість — засоби захисту можуть усунути вразливість чи зробити її менш серйозною (наприклад, якщо внутрішня мережа, що з'єднана із зовнішньою мережею, вразлива до несанкціонованого доступу, то реалізація відповідного брандмауера зробить з'єднання менш вразливим, а роз'єднання усуне цю вразливість), чи

3) вплив — засоби захисту можуть зменшити чи усунути вплив (якщо зловмисний вплив являє собою недоступність інформації, він зменшується через створення копій інформації, які надійно зберігаються в іншому місці, та готовність до активування плану неперервності бізнесу). Добре організоване реєстрування і аналізування журналів аудиту та засобів сигналізації може допомогти ранньому виявленню інциденту та знизити зловмисний вплив на бізнес.

Як і де використовують засіб захисту, може бути суттєва різниця від тієї користі, яку отримає завдяки його запровадженню. Дуже часто, загрози можуть використовувати більше ніж одну вразливість. Тому, якщо засіб захисту використовують, щоб запобігти виникненню такої загрози, він може бути спрямованим на декілька вразливостей одночасно. Зворотнє також вірно — засіб захисту, що захищає вразливість, може бути спрямованим на декілька загроз. Ці переваги слід розглядати, за можливості, під час вибору засобів захисту. Ці додаткові переваги потрібно завжди документувати, щоб мати повноту вимог безпеки, яким задовольняє будь-який засіб захисту.

Взагалі, засоби захисту можуть забезпечувати один чи більше з таких типів захисту: запобігання, стримування, виявлення, зменшення, відновлення, виправлення, моніторинг та обізнаність. Яка з цих властивостей найкраща, залежить від конкретних обставин та від призначення кожно-

го засобу. В багатьох випадках засоби захисту забезпечують більше одного типу захисту, що знову ж таки, забезпечує додаткові переваги. За можливості, треба надавати перевагу тим засобам, які мають багато переваг, ніж ті, що їх стільки не мають.

Безпека повинна завжди показувати розумний баланс щодо ефектів, згаданих вище. Якщо занадто великий акцент робиться на типі засобу захисту, малоймовірно, що загальна безпека буде ефективною. Наприклад, якщо більшість засобів стримування використовують без адекватних засобів виявлення, щоб визначити, коли стримування не спрацювало, загальна безпека не буде ефективною.

Перед реалізацією, запропоновані засоби захисту треба порівняти з наявними засобами, щоб оцінити, що треба розширяти чи оновлювати. Якщо є, то це може бути дешевше, ніж запровадження нових засобів захисту.

Під час вибору засобів захисту важливо зважувати на вартість реалізації засобів захисту відносно вартості цінностей, що захищаються, та терміни повернення інвестицій, пов'язаних зі зниженням ризику. Вартість реалізації та обслуговування засобу може бути набагато вищою, ніж вартість самого засобу, тому це треба враховувати під час вибору.

Технічні обмеження, а саме: вимоги продуктивності, керованості (вимоги обслуговування діяльності) та питань сумісності можуть заважати використанню деяких засобів захисту. В цих випадках керівники системи та безпеки мають працювати разом для прийняття оптимальних рішень. Може трапитися випадок, коли засіб захисту буде знижувати продуктивність. Знову таки, керівники системи та безпеки разом повинні прийняти рішення, що дозволить забезпечити необхідну продуктивність за умови гарантованої достатньої безпеки.

Такі аспекти, як законодавство про захист приватного життя та право можуть вимагати, щоб були наявні певні засоби захисту, тому використовується визначення незмінних базових елементів.

## 12 РОЗРОБЛЕННЯ БАЗОВОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Коли організація вирішує запровадити базову безпеку до всієї організації чи до її частин, треба розглянути такі питання.

1. Які частини організації чи систем можуть бути захищені певним базовим рівнем, а які потребують іншого, і чи може той самий базовий рівень запроваджуватись для цілої організації?
2. На який рівень безпеки має бути орієнтована базова безпека (чи різні базові безпеки)?
3. Як можуть бути визначені засоби захисту, що формують іншу базову безпеку (за потреби)?

На рисунку 4 зображено різні способи застосування базової безпеки:

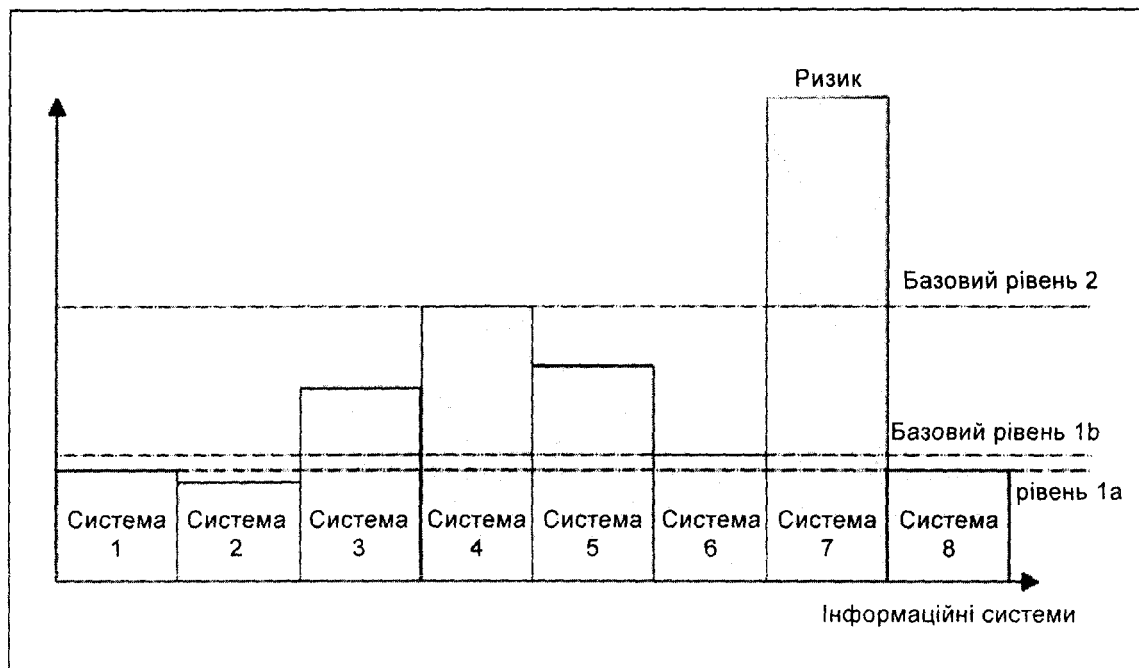


Рисунок 4 — Різні базові рівні

Перевага застосування різних базових рівнів в одній організації — це те, що більшість систем будуть захищені належним чином, тобто застосовується не надмірно малий та не надмірно великий захист (наприклад, для ІТ з базовим рівнем 1 — системи 1, 2, 6, 8 та ІТ з базовим рівнем 2 — це системи 3, 4 та 5, як зазначено на рисунку 4). Якщо інформаційні системи з різними вимогами безпеки є «насправді різними» (в тому сенсі, що більшість засобів захисту, які потрібні для захисту ІТ системи, різні), тоді для організації рекомендовано використовувати різні бази. Якщо вимоги до безпеки фундаментально відрізняються, рішення про використання базового підходу має бути переглянуто.

З іншого боку, якщо єдина відмінність між різними базовими рівнями — це та, що виникає потреба у деяких додаткових засобах захисту для формування вищих базових рівнів, тоді можливо не варто запроваджувати декілька різних базових рівнів. Якщо запроваджений тільки один базовий рівень, накладні видатки організації можуть бути значно зменшені, і кожен в організації зможе покладатися на наявність однакового рівня безпеки.

Рівень базової безпеки, на який треба орієнтуватися, звичайно, залежить від рішення, скільки рівнів базової безпеки можна логічно запровадити: один чи більше. Якщо вибрані різні базові рівні, ці рівні можуть бути встановлені достатньо точно до вимог безпеки ІТ систем, які потрібно захищати. Загалом, жоден базовий рівень не повинен бути спрямований на безпеку нижче найнижчих вимог до безпеки ІТ систем, які треба захищати (наприклад, нижче вимог ІТ системи 2 на рисунку 4). Доцільно орієнтуватись на рівень, що є достатнім для більшості (базовий рівень 1a на рисунку 4) чи всіх (базовий рівень 1b) ІТ систем, призначених для захисту. Часто доцільно орієнтуватись на найвищий рівень безпеки інформаційних систем для захисту їх базовими засобами, оскільки це зазвичай не дуже дорого, але забезпечує достатню безпеку для всіх задіяних ІТ систем. Необхідно уважно розглянути запроваджені ІТ систем для прийняття остаточного рішення, які ІТ системи будуть захищатись тим же базовим рівнем. Деякі ІТ системи багато в чому схожі за сутністю та (або) за вимогами до захисту — в цьому випадку є корисно захищати їх тим же самим базовим рівнем. З іншого боку, якщо декілька ІТ систем повністю відрізняються в своїх вимогах до захисту, дуже часто найпростіше розглядати їх окремо.

Теж саме і у випадку, якщо організація вирішує реалізовувати однаковий базовий рівень по всій організації. Ця базова безпека може бути орієнтована на три різні рівні:

- 1) низький рівень, долучаючи специфічні засоби захисту, щоб захистити всі ІТ системи з вищими вимогами;
- 2) середній рівень, долучаючи специфічні засоби захисту, щоб захистити всі ІТ системи з вищими вимогами, чи
- 3) високий рівень, що є достатнім для захисту всіх ІТ систем, передбачених для захисту базовою безпекою.

Як описано вище, середній та високий рівні базової безпеки можуть бути зручними для багатьох організацій, щоб досягти достатнього захисту, надійної безпеки по всій організації та зниження організаційних видатків. У підсумку, рішення треба приймати відповідно до політики безпеки організації та вимог ІТ систем, що розглядаються.

## 13 ВИСНОВКИ

Ця частина ISO/IEC TR 13335 описує різні способи вибору засобів захисту, які можна використовувати для досягнення базової безпеки чи для допомоги методам, описаним в ISO/IEC TR 13335-3. Ця частина ISO/IEC TR 13335 також містить огляд загальних засобів захисту, що можуть бути вибрані за допомогою будь-якого підходу, згаданому вище, та за допомогою посилання на різні довідники з базових засобів захисту, що містять детальніші описи цих засобів. Отже, описані різні способи розроблення базової безпеки організації та переваги і недоліки описаних варіантів. Ця частина ISO/IEC TR 13335 може бути використана будь-якою організацією, великою чи малою, яка хоче вибрати засоби захисту своїх інформаційних систем.

## БІБЛІОГРАФІЯ

A Code of Practice for Information Security Management	see Annex A
B ETSI Baseline Security Standard — Features and Mechanisms	see Annex B
C IT Baseline Protection Manual	see Annex C
D NIST Computer Security Handbook	see Annex D
E Medical Informatics: Security Categorization and Protection for Healthcare Information Systems	see Annex E
F TC 68 Banking and Related Financial Services	see Annex F
G Protection of sensitive information not covered by the Official Secrets Act — Recommendations for computer Workstations	see Annex G
H Canadian Handbook on Information Technology Security	see Annex H

<b>НАЦІОНАЛЬНЕ ПОЯСНЕННЯ</b>	
A Практичні правила керування інформаційною безпекою	див. додаток A
B Стандарт базової безпеки ETSI. Функції та механізми	див. додаток B
C Довідник з базового захисту IT	див. додаток C
D Посібник з комп'ютерної безпеки NIST	див. додаток D
E Медична інформатика: Категоризація безпеки та захист інформаційних систем охорони здоров'я	див. додаток E
F Банківська справа та пов'язані з нею фінансові послуги TC 68. Посібник з інформаційної безпеки	див. додаток F
G Захист контрольованої інформації, на яку не поширюється Закон про державну таємницю. Рекомендації для комп'ютерних робочих станцій	див. додаток G
H Канадський посібник з безпеки інформаційних технологій	див. додаток H

## ДОДАТОК А

### ПРАКТИЧНІ ПРАВИЛА КЕРУВАННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

(Тип: загальний)

#### Сфера застосування

BS 7799 — це багаточастинний стандарт, який містить частини:

BS 7799-1:1999 Практичні правила керування інформаційною безпекою;

BS 7799-2:1999 Специфікація систем керування інформаційною безпекою.

Ці стандарти опубліковані під авторством Департаменту стандартів Британського інституту стандартів. BS 7799-1:1999 замінює версію 1995, яка на сьогодні не чинна. BS 7799 призначений для використання директорами, керівниками та працівниками, які відповідають за ініціацію, реалізування та підтримування інформаційної безпеки в своїй організації, та може розглядатись як основа для розроблення стандартів з безпеки організації.

Версії 1999 року частин 1 та 2 були підготовлені під наглядом комітету BSI/DISC, BDD/2 «Керування інформаційною безпекою». У цих нових версіях враховано останні напрацювання в частині технологій оброблення даних, особливо у сфері мереж та комунікацій. Вони також більше акцентують на залучення бізнесу до інформаційної безпеки та відповідальність за неї. В процесі перегляду враховувались зауваження організацій з різних країн світу.

Ці документи забезпечують повний набір засобів керування, що містять найкращі приклади з інформаційної безпеки і мають бути настільки повними, наскільки це можливо. Вони мають бути єдиним джерелом посилань для визначання засобів керування, потрібних у більшості ситуацій, коли інформаційні системи використовують у виробництві та торгівлі, і тому можуть запроваджуватись великими, середніми та малими організаціями.

**Зміст BS 7799-1:1999**

- 1 Сфера застосування
- 2 Терміни та визначення понять
- 3 Політика безпеки
  - 3.1 Політика інформаційної безпеки
- 4 Організація безпеки
  - 4.1 Інфраструктура інформаційної безпеки
  - 4.2 Безпека доступу третьої сторони
  - 4.3 Аутсорсінг

**Національна примітка**

Аутсорсінг — це виконання роботи на відстані від замовника і пересилання результатів роботи електронними засобами.

- 5 Класифікація цінностей та керування ними
  - 5.1 Облік цінностей
  - 5.2 Класифікація інформації
- 6 Безпека основного персоналу
  - 6.1 Безпека у разі визначення функціональних обов'язків
  - 6.2 Навчання користувачів
  - 6.3 Реагування на порушення
- 7 Фізична безпека та безпека навколишнього середовища
  - 7.1 Безпечні зони
  - 7.2 Безпека обладнання
  - 7.3 Загальні засоби контролю
- 8 Керування діяльністю та зв'язком
  - 8.1 Методика експлуатації та обов'язки
  - 8.2 Планування та прийняття системи
  - 8.3 Захист від зловмисного програмного забезпечення
  - 8.4 Догляд
  - 8.5 Керування мережею
  - 8.6 Поводження з носіями інформації та їхня безпека
  - 8.7 Обмін даними та програмами
- 9. Контроль доступу
  - 9.1 Ділові вимоги до доступу системи
  - 9.2 Керування доступом користувачів
  - 9.3 Обов'язки користувачів
  - 9.4 Контроль доступу до мережі
  - 9.5 Контроль доступу до комп'ютера
  - 9.6 Контроль доступу до програм
  - 9.7 Моніторинг доступу до системи та її використання
  - 9.8 Мобільні обчислення та віддалена робота
- 10. Розроблення та обслуговування системи
  - 10.1 Вимоги до безпеки систем
  - 10.2 Безпека у прикладних системах
  - 10.3 Криптографічні засоби
  - 10.4 Безпека системних файлів програм.
  - 10.5 Безпека у разі розроблення та середовища, що підтримує систему
- 11. Керування неперервністю бізнесу
  - 11.1 Аспекти керування неперервністю бізнесу
- 12. Сумісність
  - 12.1 Відповідність юридичним вимогам
  - 12.2 Перегляд політики безпеки та технічної сумісності
  - 12.3 Розгляд аудиту системи

*Адреса*

BSI  
389 Chiswick High Road  
London, W4 4AL  
UK

Tel.: +44 181 996 7000

Fax: +44 181 996 7001

BS 7799 також виданий в Австралії та Новій Зеландії як AS/NZS 4444.

*Адреса*

SAA  
P.O.Box 1055  
AUS — Strathfield NSW 2135  
Australia

Tel.: +61 297 464700

Fax: +61 297 464766

BS 7799 також виданий в Швеції як SS 62 77 99.

*Адреса*

STG  
S-11289 Stockholm  
SWEDEN

Tel.: +46 8136250

Fax: +46 86186128

ДОДАТОК В

**СТАНДАРТ БАЗОВОЇ БЕЗПЕКИ ETSI. ФУНКЦІЇ ТА МЕХАНІЗМИ**

(Тип: залежний від ІТ застосування)

**Сфера застосування**

У цьому документі наведено всі особливості та механізми безпеки, що були оцінені та можуть використовуватись у стандартах ETSI. Однак цей документ тільки надає настанови з вибору та застосування конкретних механізмів безпеки, наведених у додатку. Якщо потрібна ґрунтовніша порада, наводять посилання на відповідні джерела інформації. Більше того, експерти ETSI STAG готові допомогти, якщо виникають питання та проблеми. У багатьох випадках механізми безпеки як такі офіційно не стандартизовані, але вони зареєстровані для використання. Багато з них не опубліковані з міркувань безпеки, але можуть бути використані в окремих ETSI-застосунках. Оскільки існує значна активність у сферах телекомунікацій та криптології, цей документ має переглядатись та оновлюватись регулярно.

**Зміст**

- 1 Сфера застосування
- 2 Посилання
  - 2.1 Основні особливості та механізми
  - 2.2 Специфічні системні можливості та механізми
- 3 Визначення, позначки та скорочення
  - 3.1 Визначення
  - 3.2 Скорочення
- 4 Можливості безпеки
  - 4.1 Вступ
  - 4.2 Огляд можливостей безпеки
    - 4.2.1 Автентифікація
    - 4.2.2 Конфіденційність
    - 4.2.3 Цілісність
    - 4.2.4 Контроль доступу
    - 4.2.5 Керування ключами
    - 4.2.6 Неспростовність
    - 4.2.7 Аудит безпеки

**5 Механізми безпеки****5.1 Вступ****5.2 Огляд****5.2.1 Механізми автентифікації/ідентифікації****5.2.2 Механізми конфіденційності****5.2.3 Механізми цілісності****5.2.4 Механізми контролю доступу****5.2.5 Механізми керування ключами****5.2.6 Механізми неспростовності****5.3 Формат опису****Додаток А Опис механізмів**

Механізми безпеки/автентифікація/ідентифікація

Механізми безпеки/автентифікація/ідентифікація/методи, засновані на знанні

Механізми безпеки/автентифікація/ідентифікація/методи, засновані на підтвердженні знання

Механізми безпеки/конфіденційність/шифрування

Механізми безпеки/цілісність

Механізми безпеки/контроль доступу

Механізми безпеки/керування ключами/створення спільних секретних ключів

Механізми безпеки/керування ключами/поширення відкритих ключів

**Додаток В Взаємозв'язок між послугами та механізмами безпеки****Адреса**

ETSI Secretariat

06921 Sophia Antipolis Cedex

France

Tel.: +33 9294 4200

Fax: +33 9365 4716

**ДОДАТОК С****ДОВІДНИК З БАЗОВОГО ЗАХИСТУ ІТ**

(Тип: залежний від ІТ застосування)

**Сфера застосування**

Мета базового захисту ІТ — через відповідне застосування організаційних, кадрових, інфраструктурних та технічних стандартних засобів захисту, досягнути стандарту безпеки для ІТ систем, що є адекватним та достатнім стосовно вимог до захисту середнього рівня, та може бути основою для програм, що потребують високого ступеню захисту.

З цією метою довідник з базового захисту ІТ рекомендує набори контрзаходів для типових конфігурацій ІТ, структур навколишнього середовища та організаційних заходів. Для упорядкування цього довідника Німецька агенція інформаційної безпеки використала оцінки ризику на базі відомих загроз та вразливостей і розробила пакети заходів, що відповідають цій меті. В результаті, користувачам довідника з базового захисту ІТ не треба виконувати складне аналізування базового захисту; вони мають тільки прослідкувати за тим, щоб рекомендовані засоби захисту були по-спільно та повністю впроваджені.

В той же час, це допомагає гарантувати, що інформаційна безпека в частині вимог захисту середнього рівня може бути досягнута в економний спосіб, особливо тому, що окремі стратегії безпеки систем можуть базуватися на Довідник з базового захисту ІТ. Таким чином, базовий захист ІТ стає загальною базою узгодження засобів захисту для задоволення вимог захисту середнього рівня.

**Зміст****1 Керування інформаційною безпекою****2 Застосування довідника з базового захисту ІТ****2.1 Застосування довідника з базового захисту ІТ****2.2 Визначення вимог до захисту**



- 2.3 Використання довідника з базового захисту ІТ
- 2.4 Практичні поради та допоміжні засоби
- 3 Компоненти загального базового захисту ІТ
  - 3.1 Організація
  - 3.2 Персонал
  - 3.3 Планування надзвичайних ситуацій
  - 3.4 Резервування
  - 3.5 Захист даних
  - 3.6 Захист від комп'ютерних вірусів
  - 3.7 Криптоконцепція
- 4 Інфраструктура
  - 4.1 Будівлі
  - 4.2 Прокладання кабелю
  - 4.3 Кімнати
    - 4.3.1 Офіс
    - 4.3.2 Серверна кімната
    - 4.3.3 Архіви носіїв інформації
    - 4.3.4 Кімната технічної інфраструктури
- 5 Немережні Системи
  - 5.1 DOS PC (один користувач)
  - 5.2 Системи UNIX
  - 5.3 Портативний PC
  - 5.4 DOS PC (декілька користувачів)
  - 5.5 PC Windows NT
  - 5.6 PC Windows 95
  - 5.7 Загальна мережна інформаційна система
- 6 Мережні системи
  - 6.1 Мережа на основі сервера
  - 6.2 Мережа UNIX
  - 6.3 Однорангова мережа під Windows for Workgroups
  - 6.4 Мережа Windows NT
  - 6.5 Novell Netware 3.x
  - 6.6 Novell Netware 4.x
  - 6.7 Гетерогенні мережі
  - 6.8 Керування мережею та системами
- 7 Системи передавання даних
  - 7.1 Обмін носіями даних
  - 7.2 Модем
  - 7.3 Брандмауер
  - 7.4 Електронна пошта
  - 7.5 Веб-сервер
- 8 Телекомунікації
  - 8.1 Система телекомунікацій
  - 8.2 Факс
  - 8.3 Автоповідач
  - 8.4 LAN з'єднання через ISDN
- 9 Інші компоненти ІТ
  - 9.1 Стандартне програмне забезпечення
  - 9.2 Бази даних
  - 9.3 Віддалена робота
- Каталоги засобів захисту
- Каталоги загроз
- Каталоги загроз/Таблиці засобів захисту

*Відділ стандартів*  
 DIN  
 Burggrafenstrasse 6  
 10787 Berlin  
 Germany  
 Tel.: +49 30 2601 2652  
 Fax: +49 30 2601 1723

*Адреси*  
 BSI  
 Postfach 20 03 63  
 53133 Bonn  
 Germany  
 Tel.: +49 228 9582 0  
 Fax: +49 228 9582 400

#### ДОДАТОК D

### ПОСІБНИК З КОМП'ЮТЕРНОЇ БЕЗПЕКИ NIST

(Тип: загальний)

#### Сфера застосування

Цей посібник надає допомогу організації в частині захисту комп'ютерних ресурсів (охоплюючи апаратне, програмне забезпечення та інформацію), пояснюючи важливі поняття, розрахунки вартості та взаємозв'язки засобів захисту. Він ілюструє переваги засобів захисту, основні методи чи підходи для кожного засобу та важливі міркування, пов'язані з ними.

Посібник містить загальний огляд комп'ютерної безпеки, щоб допомогти читачам зрозуміти, що їм потрібно в частині комп'ютерної безпеки, та розробити надійний підхід до вибору відповідних засобів захисту. Він не описує детальних кроків, необхідних для реалізації програми комп'ютерної безпеки, не надає детальних процедур реалізації засобів захисту, та не містить настанову з аудиту безпеки конкретних систем. У посібнику в кінці кожного розділу частин II, III та IV наведено загальні посилання, а також посилання на «how-to» («як-для») книги та статті.

Призначення цього посібника: не визначання вимог, а, швидше, обговорення переваг різних засобів захисту та ситуацій, коли їх застосування може бути корисним. Деякі вимоги для об'єднаних систем відмічено в тексті. Цей документ містить поради та настанову; про міри покарання не йдеться.

#### Зміст

- I Вступ та огляд
  - 1 Вступ
  - 2 Елементи комп'ютерної безпеки
  - 3 Ролі та обов'язки
  - 4 Загальні загрози: короткий огляд
- II Засоби керування
  - 5 Політика комп'ютерної безпеки
  - 6 Програма керування комп'ютерною безпекою
  - 7 Керування ризиками комп'ютерної безпеки
  - 8 Безпека та планування в життєвому циклі комп'ютерної системи
  - 9 Гарантування
- III Механізми експлуатації
  - 10 Питання персоналу/користувачів
  - 11 Приготування до непередбачених ситуацій та стихійних лих
  - 12 Реагування на порушення комп'ютерної безпеки
  - 13 Обізнаність, навчання та освіта
  - 14 Міркування про безпеку комп'ютерного підтримування та діяльності

- 15 Фізична безпека та безпека навколишнього середовища
- IV Технічний контроль
  - 16 Ідентифікація та автентифікація
  - 17 Контроль логічного доступу
  - 18 Журнали аудиту
  - 19 Криптографія
- V Приклад
  - 20 Оцінювання та прийнятність ризиків гіпотетичної комп'ютерної системи

*Відділ стандартів*

ANSI

11 West 42<sup>nd</sup> Street

13<sup>th</sup> floor

USA — New York, N.Y. 10036

USA

Tel.: +1 212 642 4900

Fax: +1 212 840 2298

*Адреса*

Computer systems Laboratory

NIST

Gaithersburg

MD 20899-0001

US

## ДОДАТОК Е

### МЕДИЧНА ІНФОРМАТИКА: КАТЕГОРИЗАЦІЯ БЕЗПЕКИ ТА ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ОХОРОНИ ЗДОРОВ'Я

(Тип: залежний від ІТ застосування)

#### Сфера застосування

Цей європейський пробний стандарт визначає метод категоризації автоматизованих інформаційних систем для охорони здоров'я в контексті безпеки. Безпеку розглядали у значенні зберігання на припустимому рівні доступності даних, конфіденційності та цілісності. Для кожної категорії систем визначено належний набір захисних вимог, придатний для рівня ризиків, властивого цій категорії.

Цей європейський пробний стандарт застосовний для всіх автоматизованих інформаційних систем, що обробляють інформацію, яка стосується охорони здоров'я. Вони охоплюють системи, які прямо сприяють догляду за хворими, наприклад, обробляють результати лабораторних тестів; але також охоплюють статичні системи, а також адміністративні системи, що забезпечують підтримання функціонування закладу охорони здоров'я самого по собі, наприклад виплата зарплати, кадрові, планові та фінансові системи. Однак цей європейський пробний стандарт не поширюється на системи, де конфіденційність вважається неважливою, тобто інформація є загальним надбанням. Користувачами цього пробного стандарту є споживачі/постачальники безпечних інформаційних систем для охорони здоров'я та розробники/виробники безпечних інформаційних систем для цієї сфери. Запровадження положень цього європейського пробного стандарту розцінюється як дотримання керівництвом національних та європейських законів, а також очікування громадськості на високі стандарти безпеки інформації в сфері охорони здоров'я.

#### Зміст

- 1 Сфера застосування
- 2 Нормативні посилання
- 3 Визначення
- 4 Скорочення
- 5 Категоризація інформаційних систем для охорони здоров'я
- 6 Профіль захисту І (Базові вимоги)

- 7 Профіль захисту II
  - Базові вимоги
  - Вищі вимоги
- 8 Профіль захисту III
  - Базові вимоги
  - Вищі вимоги
- 9 Профіль захисту IV
  - Базові вимоги
  - Вищі вимоги
- 10 Профіль захисту V
  - Базові вимоги
  - Вищі вимоги
- 11 Профіль захисту VI
  - Базові вимоги
  - Вищі вимоги

Додаток А (довідковий) Підхід до категоризації систем

Додаток В (довідковий) Як використовувати цей європейський стандарт

Додаток С (довідковий) Приклади категоризації інформаційних систем

Додаток D (довідковий) Категоризація інформаційних систем

Додаток Е (довідковий) Джерела загрози

Додаток F (довідковий) Література

Адреса

CEN TC 251

Rue de Stassart 36

1050 Brussels

Belgium

#### ДОДАТОК F

### БАНКІВСЬКА СПРАВА ТА ПОВ'ЯЗАНІ З НЕЮ ФІНАНСОВІ ПОСЛУГИ ТК 68 (ТС 68) НАСТАНОВА З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

(Тип: залежний від ІТ застосування)

#### Сфера застосування

Фінансові установи все більше покладаються на інформаційні технології (ІТ) для ефективного керування бізнесом. Керування ризиками є головним для сегмента фінансових послуг. Ці установи керують ризиками шляхом використовування обережного ведення бізнесу, уважного укладання угод, страхування, та використовування відповідних механізмів безпеки.

Є потреба керувати інформаційною безпекою в фінансових установах комплексно. Цей технічний звіт не призначений для забезпечення загального рішення для всіх ситуацій. Кожний випадок має бути вивчений по суті, щоб визначитись з відповідними діями. Цей звіт призначений для розроблення настанови, а не конкретних рішень.

Метою цього технічного звіту є:

- структура програми інформаційної безпеки;
- настанова з вибору засобів захисту, прийнятних для обережної практики ведення бізнесу.
- забезпечення сумісності з наявними стандартами, а також об'єктивними та надійними критеріями безпеки роботи, яка щойно започаткована.

Цей технічний звіт призначений для використовування фінансовими установами всіх розмірів та типів, які бажають реалізувати розумну та комерційно обґрунтовану програму безпеки. Він також буде корисним для постачальників послуг для фінансових установ. Цей звіт також може слугувати основним документом для викладачів та видавців, що працюють у фінансовій сфері.

## **Зміст**

- 1 Вступ
- 2 Керування інформаційною безпекою
- 3 Корпоративна політика інформаційної безпеки
- 4 Організація інформаційної безпеки
  - 4.1 Зобов'язання
  - 4.2 Ролі та обов'язки
- 5 Аналізування ризиків
  - 5.1 Вступ
  - 5.2 Ілюстрований процес аналізування ризиків
  - 5.3 Загрози
  - 5.4 Вразливості
  - 5.5 Категорії ризиків
  - 5.6 Визначення та аналіз ділових функцій
  - 5.7 Процес оцінювання ризиків.
- 6 Рекомендації інформаційної безпеки
  - 6.1 Прийнятність ризиків
- 7 Вибір засобів захисту
  - 7.1 Класифікація інформації
  - 7.2 Контролювання логічного доступу
  - 7.3 Журнали аудиту
  - 7.4 Контролювання змін
- 8 Реалізація засобів захисту
  - 8.1 Комп'ютери
  - 8.2 Мережі
  - 8.3 Програмне забезпечення
  - 8.4 Голосове, телефонне та інше обладнання
  - 8.5 Передавання факсів та зображень
  - 8.6 Електронна пошта
  - 8.7 Паперові документи
  - 8.8 Мікроформи та інші носії даних
  - 8.9 Карти фінансових транзакцій
  - 8.10 Банкомати
  - 8.11 Електронні гроші та перекази
  - 8.12 Перевіряння
  - 8.13 Електронна комерція
  - 8.14 Електронні гроші
  - 8.15 Різне
  - 8.16 Страхування
  - 8.17 Аудит
  - 8.18 Відповідність правовим нормам
  - 8.19 Планування відновлення після стихійних лих
  - 8.20 Зовнішні постачальники послуг
  - 8.21 Криптографічна діяльність
  - 8.22 Секретність
  - 8.23 Реалізація криптографічних засобів захисту
- 9 Інформування про безпеку
  - 9.1 Інформування про інформаційну безпеку
  - 9.2 Людські чинники
- 10 Підтримування безпеки
  - 10.1 Обслуговування
  - 10.2 Сумісність безпеки
  - 10.3 Моніторинг
  - 10.4 Реагування на порушення
- 11 Посилання

Додаток А Зразки документів  
 Додаток В Зразок базової безпеки  
*Адреса*  
 ISO/ TC 68/SC2 Secretariat  
 Post Office Box 11  
 Annapolis Junction  
 MD 20701  
 USA  
 Tel.: +1 301 688 3586  
 Fax: +1 301 192 1019

## ДОДАТОК G

**ЗАХИСТ КОНТРОЛЬОВАНОЇ ІНФОРМАЦІЇ,  
 НА ЯКУ НЕ ПОШИРЮЄТЬСЯ ЗАКОН УКРАЇНИ «ПРО ДЕРЖАВНУ ТАЄМНИЦЮ»  
 РЕКОМЕНДАЦІЇ ДЛЯ КОМП'ЮТЕРНИХ РОБОЧИХ СТАНЦІЙ**

(Тип: загальний)

**Сфера застосування**

Цей документ поширюється на заходи гарантування захисту контрольованої інформації, на яку не поширюється Закон України «Про державну таємницю», та яка обробляється чи зберігається комп'ютерними засобами, і запровадження цих законів різними посадовими особами організації. Ці рекомендації стосуються зокрема такого:

- дорогого програмного забезпечення, пошкодження чи розкриття якого може поставити організацію у скрутне становище,
- не можна розкривати інформацію специфічної конфіденційності або інформацію з обмеженим доступом згідно з вимогами до збереження професійної таємниці. Для інформації вищого рівня секретності, такої як специфічна секретна інформація, відповідні органи мають посилити заходи, рекомендовані в цьому документі.

Ці органи мають на основі цих рекомендацій розробити свої внутрішні інструкції.

**Зміст**

- 0 Вступ
- 1 Сфера застосування
- 2 Адміністрування та організація безпеки
  - 2.1 Учасники забезпечення безпеки та їхні ролі
  - 2.2 Процедури
- 3 Фізична безпека
  - 3.1 Приміщення
  - 3.2 Встановлення комп'ютерного обладнання
  - 3.3 Контролювання доступу персоналу до апаратного забезпечення
  - 3.4 Контролювання доступу персоналу до будівель
- 4 Безпека персоналу
  - 4.1 Обов'язки та процедури
  - 4.2 Навчання та підвищення обізнаності
- 5 Безпека документів
  - 5.1 Оброблення та захист інформації
  - 5.2 Оброблення та захист носіїв даних
- 6 Безпека комп'ютерів
  - 6.1 Комп'ютерне обладнання
  - 6.2 Контроль доступу
  - 6.3 Програмне забезпечення
  - 6.4 Файли

- 6.5 Обслуговування
  - 6.6. Тимчасовий ремонт
  - 6.7 Нагляд та перевіряння
  - 7 Збереження (резервування) та надзвичайні дії
    - 7.1 Процедури збереження (резервування) файлів даних
    - 7.2 Процедури збереження програм
    - 7.3 Надзвичайні дії — Загальні збої
    - 7.4 Надзвичайні дії — Логічні напади
    - 7.5 Надзвичайні дії — Катастрофи
  - 8 Безпека комунікацій
    - 8.1 Криптографічна безпека
    - 8.2 Безпека каналів передавання даних та отримання доступів
  - 9 Керування конфігурацією
- Додаток А (довідковий) Прийняття зобов'язань
- Адреса  
AFNOR  
Tour Europe  
92049 Paris La Défense Cedex  
France  
Tel.: +33 1 4291 5555  
Fax: +33 1 4291 5656

#### ДОДАТОК Н

### КАНАДСЬКИЙ ПОСІБНИК З БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

(Тип: загальний)

#### Сфера застосування

Цей посібник допомагає забезпечувати захист комп'ютерних ресурсів (охоплюючи апаратне, програмне забезпечення та інформацію), пояснює важливі поняття, наводить розрахунки вартості та взаємозв'язані засоби захисту. Він ілюструє переваги засобів захисту, основні методи чи підходи для кожного засобу та важливі міркування, пов'язані з ними.

Посібник містить загальний огляд комп'ютерної безпеки, щоб допомогти читачам зрозуміти, що їм потрібно в частині комп'ютерної безпеки, та розробити надійний підхід до вибору відповідних засобів захисту. Він не описує детальних кроків, необхідних для реалізації програми комп'ютерної безпеки, не надає детальних процедур реалізації засобів захисту та не містить настанову з аудиту безпеки конкретних систем. У посібнику в кінці кожного розділу частин II, III, та IV наведено загальні посилання, а також посилання на "how-to" ("як-для") книги та статті.

Призначення цього посібника: не означення вимог, а, швидше, обговорення переваг різних засобів захисту та ситуацій, коли їх застосування може бути корисним. Деякі вимоги для об'єднаних систем відмічено в тексті. Цей документ містить поради та настанову; про міри покарання не йдеться.

#### Зміст

- I Вступ та огляд
  - 1 Вступ
  - 2 Елементи інформаційної безпеки
  - 3 Ролі та обов'язки
  - 4 Загальні загрози: короткий огляд
- II Засоби керування
  - 5 Політика інформаційної безпеки
  - 6 Програма керування інформаційною безпекою
  - 7 Керування ризиками інформаційною безпеки

8 Планування інформаційної безпеки в життєвому циклі інформаційної системи

9 Гарантування

III Експлуатаційні засоби захисту

10 Питання персоналу/користувачів

11 Приготування до непередбачених ситуацій та катастроф ІТ

12 Інформаційна безпека в частині реагування на порушення

13 Усвідомленість інформаційної безпеки у сфері, навчання та освіти

14 Міркування щодо безпеки в комп'ютерному підтримуванні та діяльності

15 Фізична безпека та безпека навколишнього середовища ІТ

IV Технічне контролювання

16 Ідентифікація та автентифікація

17 Контролювання логічного доступу

18 Журнали аудиту

19 Криптографія

V Приклад

20 Оцінювання та прийнятність ризиків гіпотетичної комп'ютерної системи

*Відділ стандартів*

SCC

45 O'Connor Street

Suite 1200

Ottawa, Ontario K1P 6N7

Canada

Tel.: +1 613 238 3222

Fax: +1 613 995 4564

*Адреса*

Communications Security Establishment

P.O. Box 9703, Terminal

Ottawa, Ontario K1G 3Z4

Canada

---

УКНД 35.040

**Ключові слова:** аналіз ризиків, ідентифікація, автентичність, ризики безпеки, конфіденційність, цінність, елементи безпеки, процеси керування безпекою ІТ, корпоративна політика, інформаційна безпека, загроза, вразливість, засоби захисту.

---