НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ ЛАНЦЮГА ПОСТАЧАННЯ

Вимоги

(ISO 28000:2007, IDT)

ДСТУ ISO 28000:2008

Видання офіційне

БЗ № 8–2008/393

Київ
ДЕРЖСПОЖИВСТАНДАРТ УКРАЇНИ
2011

ПЕРЕДМОВА

1 ВНЕСЕНО: Державне підприємство «Науково-дослідний інститут метрології вимірювальних і управляючих систем» (ДП «НДІ «Система») спільно з Технічним комітетом стандартизації «Системи управління якістю, довкіллям та безпечністю харчових продуктів» (ТК 93)

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **Л. Віткін,** канд. техн. наук; **В. Горопацький,** канд. фіз.-мат. наук; **І. Єршова,** канд. техн. наук; **О. Мокрицька; В. Паракуда,** канд. техн. наук; **А. Сухенко** (науковий керівник); **Ю. Тройнін**

2 НАДАНО ЧИННОСТІ: наказ Держспоживстандарту України від 4 серпня 2008 р. № 268 з 2009–01–01, зі зміною, внесеною наказом Держспоживстандарту України від 27.03.2009 № 124

3 Національний стандарт відповідає ISO 28000:2007 Specification for security management systems for the supply chain (Вимоги до системи управління безпекою ланцюга постачання)

Ступінь відповідності — ідентичний (IDT)
Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є тотожний переклад ISO 28000:2007 Specification for security management systems for the supply chain (Технічні вимоги до систем управління безпекою ланцюга постачання).

Технічний комітет, відповідальний за цей стандарт, — ТК 93 «Системи управління якістю, довкіллям та безпечністю харчових продуктів» (підкомітет ПК 93/1 «Системи управління якістю»).

У стандарті зазначено вимоги, які відповідають чинному законодавству України.

До стандарту внесено такі редакційні зміни:

— слова «цей міжнародний стандарт» замінено на «цей стандарт»;

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

— уточнено назву національного стандарту;

— вилучено «Передмову» до ISO 28000:2007 як таку, що безпосередньо не стосується цього стандарту;

— у розділі «Бібліографія» наведено «Національне пояснення», виділене рамкою.

Додаток А — довідковий.

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

ВСТУП до ISO 28000:2007

Цей стандарт розроблено у відповідь на потребу промисловості у стандарті щодо управління безпекою. Його основна ціль — підвищити безпеку ланцюгів постачання. Цей стандарт є стандартом щодо управління найвищого рівня, який дає змогу організації розробити загальну систему управління безпекою ланцюга постачання. Він вимагає від організації оцінювати середовище безпеки, у якому вона функціює, і визначати, чи запроваджено відповідні заходи безпеки, і чи існують вже інші нормативні вимоги, яких дотримується організація. Якщо потреби безпеки ідентифіковано за допомогою цього процесу, організація має запровадити механізми та процеси, щоб задовольняти ці потреби. Оскільки за своїм характером ланцюги постачання є динамічними, деякі організації, що керують багатьма ланцюгами постачання, можуть розглянути діяльність своїх надавачів послуг стосовно задоволення відповідних стандартів державного рівня чи стандартів ISO щодо безпеки ланцюга постачання як умови введення їх у цей ланцюг постачання, для того щоб спростити управління безпекою, як зображено на рисунку 1.

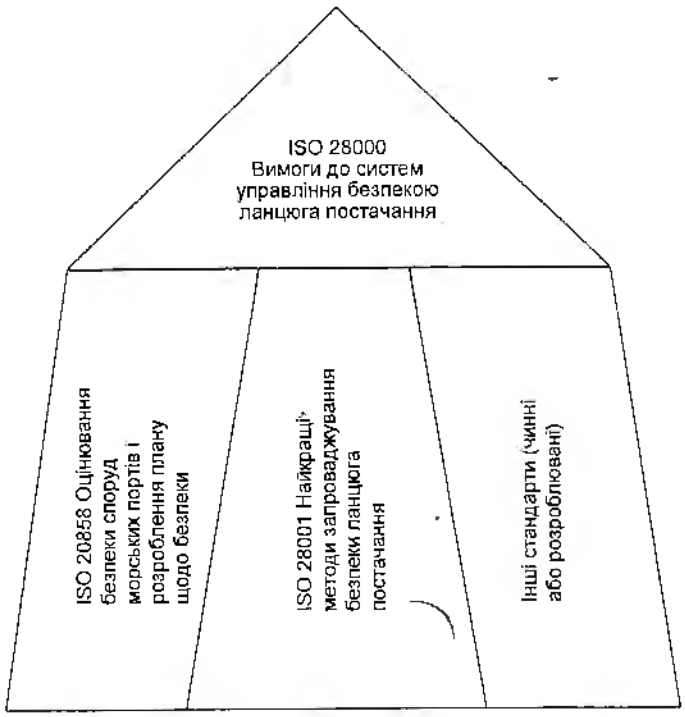

Рисунок 1 — Зв'язок між ISO 28000 та іншими відповідними стандартами

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ ЛАНЦЮГА ПОСТАЧАННЯ

Вимоги

СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ЦЕПИ ПОСТАВКИ

Требования

SPECIFICATION FOR SECURITY MANAGEMENT SYSTEMS FOR THE SUPPLY CHAIN

Чинний від 2009–01–01

1 СФЕРА ЗАСТОСУВАННЯ

Цей стандарт установлює вимоги до системи управління безпекою, зокрема стосовно аспектів, які є критичними щодо гарантування безпеки ланцюга постачання. Управління безпекою пов'язане з багатьма іншими аспектами керування підприємством. Ці аспекти охоплюють усі контрольовані організацією або залежні від неї види діяльності, які впливають на безпеку ланцюга постачання. Ці інші аспекти треба розглядати у повному обсязі, де і коли вони чинять вплив на управління безпекою, зокрема переміщення виробів по всьому ланцюгу постачання.

Цей стандарт застосовний до організацій будь-якого розміру, від малих до транснаціональних, залучених до виготовляння, обслуговування, зберігання чи транспортування на будь-якій стадії виробництва чи ланцюга постачання, які мають намір:

a) розробити, запровадити, підтримувати та поліпшувати систему управління безпекою;

b) забезпечувати відповідність проголошеній політиці у сфері управління безпекою;

c) демонструвати іншим цю відповідність;

d) сертифікувати/зареєструвати свою систему управління безпекою акредитованим незалежним органом сертифікації;

e) самостійно визначити та задекларувати відповідність цьому стандарту.

Стосовно деяких вимог цього стандарту є законодавчі та нормативні кодекси.

Цей стандарт не вимагає подвійного підтвердження відповідності.

Організації, які обирають сертифікацію третьою стороною, можуть у подальшому демонструвати, що вони значною мірою сприяють безпеці ланцюга постачання.

2 НОРМАТИВНІ ПОСИЛАННЯ

Нормативних посилань нема. Цей розділ долучено для того, щоб нумерація розділів була аналогічною нумерації в інших стандартах на системи управління.

Видання офіційне

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті використано такі терміни та визначення понять:

3.1 засіб виробництва (*facility*)

Завод, устаткування, майно, будівлі, транспортні засоби, судна, портові споруди й інші інфраструктурні чи заводські об'єкти та пов'язані з ними системи, призначені для виконання окремих виробничих функцій чи надання окремих послуг, що їх можна визначити кількісно.

Примітка. Це визначення охоплює будь-яку комп'ютерну програму, яка є вирішально важливою для гарантування безпеки та застосовування управління безпекою

3.2 безпека (*security*)

Захищеність від навмисних, несанкційованих дій, спрямованих на пошкодження ланцюга постачання або завдання шкоди його зацікавленим сторонам

3.3 управління безпекою (*security management*)

Систематичні та скоординовані дії та практика, за допомогою яких організація оптимально керує своїми ризиками, а також пов'язаними з цим потенційними загрозами та впливами

3.4 ціль у сфері управління безпекою (*security management objective*)

Конкретний результат або досягнення, необхідні з погляду безпеки, для того щоб задовольняти політику у сфері управління безпекою.

Примітка. Важливо, щоб ці результати безпосередньо чи опосередковано стосувалися постачання продукції чи надання послуг підприємством своїм замовникам чи кінцевим користувачам

3.5 політика у сфері управління безпекою (*security management policy*)

Загальні наміри та скерованість організації щодо безпеки та структури контролювання пов'язаних із безпекою процесів і діяльності, які випливають з політики організації та нормативних вимог і які узгоджено з ними

3.6 програми управління безпекою (*security management programmes*)

Засоби досягнення цілі у сфері управління безпекою

3.7 завдання у сфері управління безпекою (*security management target*)

Конкретний рівень дієвості, необхідний для досягнення цілі у сфері управління безпекою

3.8 зацікавлена сторона (*stakeholder*)

Особа чи суб'єкт, які особисто зацікавлені в результативності, успішності організації чи у впливі її діяльності.

Примітка. Прикладами є замовники, акціонери, фінансисти, страховики, інспектори, законодавчо засновані органи, роботодавці, підрядники, постачальники, організації з працевлаштування або суспільство

3.9 ланцюг постачання (*supply chain*)

Пов'язана сукупність ресурсів і процесів, яка починається з придбання сировини, і далі це реалізують постачанням продукції чи послуг кінцевому користувачеві різними способами транспортування.

Примітка. Ланцюг постачання охоплює торговців, виробничі об'єкти, організаторів матеріально-технічного забезпечення, внутрішні центри розподіляння, дистриб'юторів, оптовиків та інших суб'єктів господарювання, які наближають товар до кінцевого користувача

3.9.1 низхідний потік (*downstream*)

Стосується дій, процесів і переміщень вантажу в ланцюзі постачання, які виникають після того, як вантаж виходить з-під безпосередньо робочого контролю організації, охоплюючи, але не обмежуючись цим, страхування, фінансування, керування даними, а також пакування, зберігання та перевезення вантажу

3.9.2 висхідний потік (*upstream*)

Стосується дій, процесів і переміщень вантажу в ланцюзі постачання, які виникають перед тим, як вантаж потрапляє під безпосередній робочий контроль організації, охоплюючи, але не обмежуючись цим, страхування, фінансування, керування даними, а також пакування, зберігання та перевезення вантажу

3.10 найвище керівництво (*top management*)

Особа чи група осіб, яка спрямовує та контролює організацію на найвищому рівні.

Примітка. Найвище керівництво, особливо у великій транснаціональній організації, може не бути особисто залученим, як описано в цьому стандарті; проте потрібно, щоб відповідальність найвищого керівництва по всьому ієрархічному ланцюгу керування була очевидною

3.11 постійне поліпшування (*continual improvement*)

Повторюваний процес удосконалювання системи управління безпекою задля досягнення поліпшень загального результату діяльності з безпеки, узгодженої з політикою організації у сфері безпеки.

4 ЕЛЕМЕНТИ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ

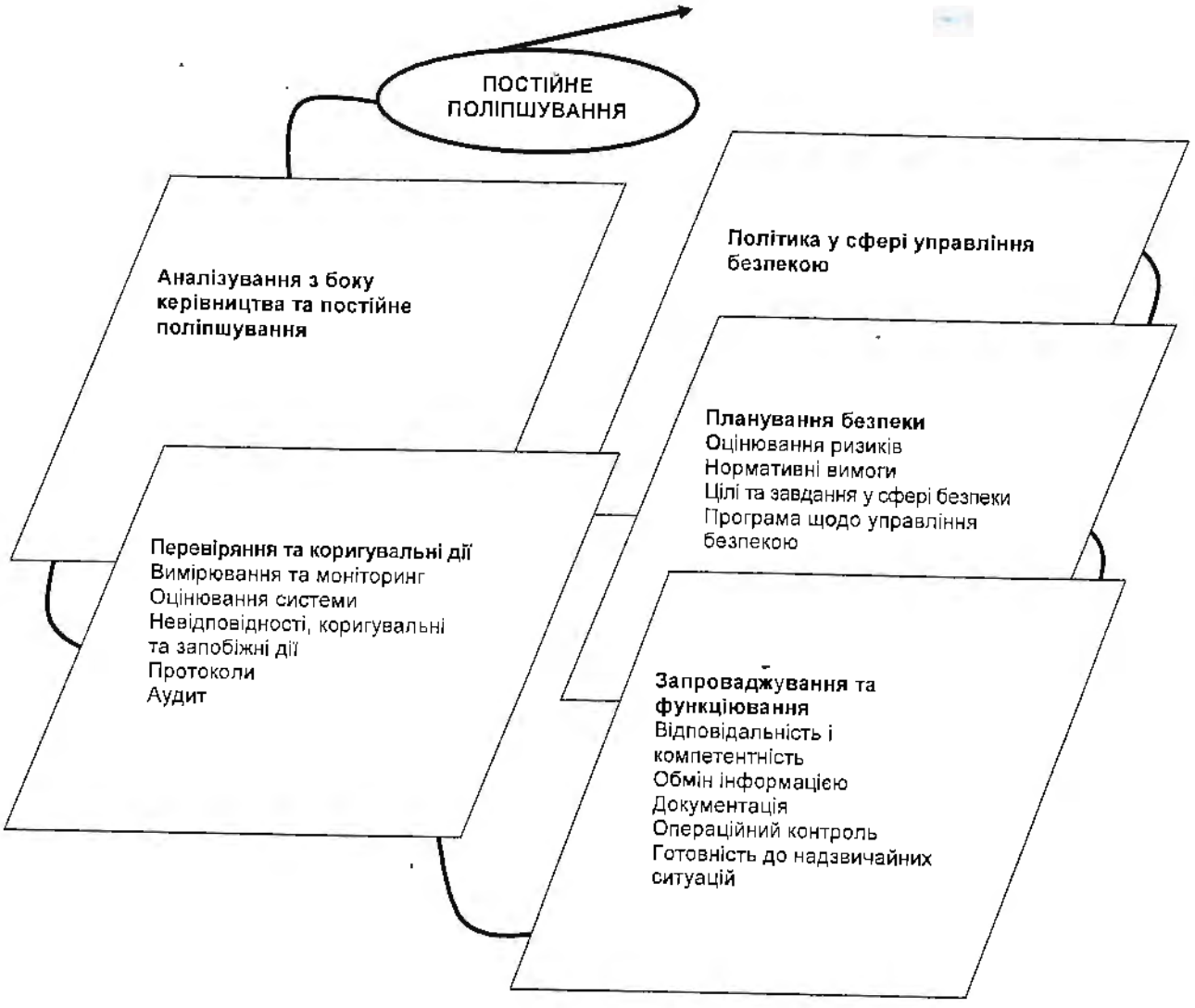

Рисунок 2 — Елементи системи управління безпекою

4.1 Загальні вимоги

Організація повинна розробити, задокументувати, запровадити, підтримувати та постійно поліпшувати результативну систему управління безпекою, щоб визначати загрози безпеці, оцінювати ризики та контролювати й пом'якшувати їхні наслідки.

Організація повинна постійно поліпшувати свою результативність відповідно до вимог, установлених у розділі 4.

Організація повинна визначити сферу застосовування своєї системи управління безпекою. Якщо для будь-якого процесу, який впливає на відповідність цим вимогам, організація вибирає стороннього виконавця, вона повинна забезпечити, щоб такі процеси були контрольованими. У системі управління безпекою потрібно ідентифікувати необхідні заходи контролю та відповідальність за процеси, передані сторонньому виконавцеві.

4.2 Політика у сфері управління безпекою

Найвище керівництво організації повинне затвердити загальну політику у сфері управління безпекою. Потрібно, щоб ця політика

a) була узгоджена з іншими політиками організації;

b) була основою для формування конкретних цілей, завдань і програм у сфері управління безпекою;

c) була узгоджена із загальним механізмом організації у сфері управління ризиками та загрозами безпеці;

d) була відповідною щодо загроз для організації та характеру й масштабу її робіт;

e) чітко проголошувала загальні/основні цілі у сфері управління безпекою;

f) мала зобов'язання щодо постійного поліпшування процесу управління безпекою;

g) мала зобов'язання щодо забезпечення відповідності чинному застосовному законодавству, нормативним і статутним вимогам, а також іншим вимогам, що їх організація зобов'язується виконувати;

h) була схвалена найвищим керівництвом;

i) була задокументована, запроваджена та підтримувана;

j) була повідомлена всім відповідним працівникам і третім сторонам, зокрема підрядникам і відвідувачам, з тим, щоб ці особи були обізнані зі своїми особистими обов'язками, пов'язаними з управлінням безпекою;

k) була доступною для зацікавлених сторін в усіх відповідних випадках;

l) була проаналізована в разі придбання інших організацій або злиття з іншими організаціями чи за інших змін у сфері господарювання організації, які можуть впливати на цілісність або відповідність системи управління безпекою.

Примітка. Організації можуть вирішити мати докладну політику у сфері управління безпекою для внутрішнього використовування, яка б забезпечувала достатньою інформацією та вказівками, щоб задіяти систему управління безпекою (частини якої можуть бути конфіденційними), а також мати узагальнену (не конфіденційну) версію з основними цілями для розповсюдження своїм зацікавленим сторонам.

4.3 Загальне оцінювання та планування ризиків

4.3.1 *Загальне оцінювання ризиків*

Організація повинна розробити та підтримувати методики постійної ідентифікації та загального оцінювання загроз безпеці та загроз і ризиків, пов'язаних з управлінням безпекою, а також визначання та вжиття необхідних заходів адміністративного контролю. Визначання, загальне оцінювання та методи контролювання загроз безпеці та ризиків мають, принаймні, відповідати характеру та масштабу робіт. Потрібно, щоб це загальне оцінювання враховувало ймовірність події та всі її наслідки, зокрема:

a) загрози та ризики фізичної відмови, наприклад, функційну відмову, випадкове пошкодження, навмисне пошкодження або терористичні чи кримінальні дії;

b) виробничі загрози та ризики, зокрема контроль безпеки, людські чинники та інші види робіт, які впливають на результативність, стан або безпечність діяльності організації;

c) події у природному середовищі (буревії, повені тощо), які можуть призвести до неефективності заходів і устаткування у сфері безпеки;

d) неконтрольовані організацією чинники, наприклад, відмови в устаткованні та послугах сторонніх постачальників;

e) зацікавленим сторонам загрози і їхній ризик, наприклад, недотримання нормативних вимог або заподіяння шкоди репутації чи престижу торгової марки;

f) проектування та встановлення устаткування, пов'язаного з безпекою, зокрема його заміну, технічне обслуговування тощо;

g) опрацьовування й передавання інформації та даних і їх оприлюднення;

h) загрозу для безперервності робіт.

Організація повинна забезпечувати, щоб результати цих загальних оцінок і заходів контролю було враховано та, в усіх відповідних випадках, щоб вони були вхідними даними для:

a) цілей і завдань у сфері управління безпекою;

b) програм управління безпекою;

c) установлення вимог до проектування, складання специфікацій та монтування;

d) визначання відповідних ресурсів, зокрема кількості штатного персоналу;

e) визначання потреб у навчанні персоналу та визначання навичок (див. 4.4.2);

f) розробляння заходів операційного контролю (див. 4.4.6);

g) загальної структурної основи системи управління ризиками в організації та унайменшення загроз.

Організація повинна задокументувати та постійно актуалізовувати зазначену вище інформацію.

Потрібно, щоб застосовувана в організації методологія визначання та загального оцінювання загроз та ризиків

a) була визначена стосовно сфери діяльності, характеру та строків, щоб забезпечувати скорішу її випереджувальність (проактивність), аніж виправність (реактивність);

b) охоплювала збирання інформації, пов'язаної із загрозами безпеці та ризиками;

c) передбачала класифікацію загроз і ризиків, а також ідентифікацію тих, яких потрібно уникати, усувати чи контролювати;

d) передбачала моніторинг дій, щоб забезпечувати результативність і своєчасність їх реалізації (див. 4.5.1).

4.3.2 ***Правові, статутні та інші нормативні вимоги у сфері безпеки***

Організація повинна розробити, запровадити та підтримувати методику

a) визначання та забезпечення доступу до застосовних правових вимог та інших вимог, пов'язаних із загрозами безпеці та ризиками, які організація зобов'язується дотримувати;

b) визначання, як ці вимоги застосовують до її загроз безпеці та ризиків.

Організація повинна актуалізовувати цю інформацію. Вона повинна подавати відповідну інформацію про правові та інші вимоги своїм працівникам та іншим відповідним третім сторонам, зокрема підрядникам.

4.3.3 ***Цілі у сфері управління безпекою***

Організація повинна розробити, запровадити та підтримувати задокументовані цілі у сфері управління безпекою для відповідних підрозділів і рівнів в організації. Потрібно, щоб цілі випливали з політики та були узгодженими з нею. Під час розробляння та аналізування своїх цілей організація повинна враховувати

a) правові, статутні та інші нормативні вимоги у сфері безпеки;

b) загрози та ризики, пов'язані з безпекою;

c) технологічні та інші можливості вибору;

d) фінансові, технічні та бізнесові вимоги;

e) погляди відповідних зацікавлених сторін.

Потрібно, щоб цілі у сфері управління безпекою

a) були узгодженими із зобов'язанням організації щодо постійного поліпшування;

b) були кількісно поданими (там, де це практично можливо);

c) були повідомлені всім відповідним працівникам та третім сторонам, зокрема підрядникам, з тим, щоб ці особи були обізнаними зі своїми особистими обов'язками;

d) періодично аналізували, щоб забезпечувати впевненість у тому, що вони залишаються відповідними та узгодженими з політикою у сфері управління безпекою.

У разі необхідності потрібно вносити відповідні зміни до цілей у сфері управління безпекою.

4.3.4 ***Завдання у сфері управління безпекою***

Організація повинна розробити, запровадити та підтримувати задокументовані завдання у сфері управління безпекою, які відповідають потребам організації. Потрібно, щоб завдання випливали з цілей у сфері управління безпекою та були узгодженими з ними.

Потрібно, щоб ці завдання

a) мали належний рівень докладності;

b) були конкретними, вимірними, досяжними, відповідними та реальними за строками (коли це практично можливо);

c) були повідомлені всім відповідним працівникам і третім сторонам, зокрема підрядникам, з тим, щоб ці особи були обізнаними зі своїми особистими обов'язками;

d) періодично аналізували, щоб забезпечувати впевненість у тому, що вони залишаються відповідними та узгодженими з цілями у сфері управління безпекою. У разі необхідності потрібно вносити відповідні зміни до завдань.

4.3.5 ***Програми у сфері управління безпекою***

Організація повинна розробити, запровадити та підтримувати програми управління безпекою для досягання своїх цілей та виконання своїх завдань.

Програми потрібно оптимізовувати з подальшим установленням пріоритетів, а організація повинна передбачити заходи щодо ефективної та економічно вигідної реалізації цих програм

Для цього потрібно розробити документацію, у якій описано

a) призначені відповідальність і повноваження щодо досягнення цілей та виконання завдань у сфері управління безпекою;

b) засоби та строки, потрібні для досягнення цілей і виконання завдань у сфері управління безпекою.

Програми управління безпекою потрібно періодично аналізувати, щоб забезпечувати впевненість у тому, що вони залишаються результативними та узгодженими з цілями та завданнями. У разі необхідності до програм потрібно вносити відповідні зміни.

4.4 Запроваджування та функціювання

4.4.1 ***Структура, повноваження та відповідальність щодо управління безпекою***

Організація повинна розробити та підтримувати організаційну структуру із зазначенням обов'язків, відповідальності та повноважень, узгоджену з досягненням своєї політики, цілей, виконанням завдань і програм у сфері управління безпекою.

Ці обов'язки, відповідальність і повноваження потрібно визначити, задокументувати та повідомити тим, хто відповідає за запроваджування та підтримування.

Найвище керівництво повинне надавати докази виконання свого зобов'язання щодо розроблляння та запроваджування системи (процесів) управління безпекою та постійного поліпшування її результативності через

a) призначання представника найвищого керівництва, який, незалежно від інших обов'язків, повинен відповідати за загальне розроблляння, підтримування, документування та запроваджування системи управління безпекою в організації;

b) призначання представника(-ів) керівництва з наданням необхідних повноважень, щоб забезпечувати реалізацію цілей і завдань;

c) визначення та проведення моніторингу вимог і очікувань зацікавлених сторін організації та виконання належних і своєчасних дій, щоб керувати цими очікуваннями;

d) забезпечування наявності потрібних ресурсів;

e) враховування можливого несприятливого впливу політики, цілей, завдань, програм тощо у сфері управління безпекою на інші аспекти функціювання організації;

f) забезпечування того, щоб будь-які програми з безпеки, що їх формують інші підрозділи організації, доповнювали систему управління безпекою;

g) повідомляння працівникам організації важливості виконання вимог управління безпекою, з тим, щоб відповідати своїй політиці;

h) забезпечування того, щоб пов'язані з безпекою загрози та ризики було належно оцінено та враховано в загальних оцінках загроз і ризиків для організації;

i) забезпечування досягненості цілей, виконання завдань і програм у сфері управління безпекою.

4.4.2 ***Компетентність, підготовленість і обізнаність***

Організація повинна забезпечувати, щоб персонал, відповідальний за проектування і функціювання устаткування та процесів у сфері безпеки та управління ними, був належним чином компетентний з погляду освіти, підготовленості та/або досвіду. Організація повинна розробити та підтримувати методики для забезпечення того, щоб особи, які працюють в організації чи за її дорученням, були обізнані з

a) важливістю дотримання відповідності політиці та методикам у сфері управління безпекою, а також вимогам системи управління безпекою;

b) своїми обов'язками та відповідальністю щодо досягнення належності політиці та методикам у сфері управління безпекою, а також вимогам системи управління безпекою, зокрема вимогам щодо готовності до надзвичайних ситуацій і реагування на них;

c) потенційними наслідками для безпеки організації через недотримання від установлених робочих методик.

Потрібно вести протоколи стосовно компетентності та підготовленості персоналу.

4.4.3 ***Обмін інформацією***

Організація повинна мати методики забезпечення обміну належною інформацією стосовно управління безпекою з відповідними працівниками, підрядниками та іншими зацікавленими сторонами.

Треба належним чином враховувати конфіденційність деякої інформації, пов'язаної з безпекою, перед її поширенням.

4.4.4 ***Документація***

Організація повинна розробити та підтримувати документацію системи стосовно управління безпекою, яка охоплює, але не обмежується цим:

a) політику, цілі та завдання у сфері безпеки;

b) опис сфери застосовування системи управління безпекою;

c) опис основних елементів системи управління безпекою та їх взаємодію, а також посилання на пов'язані з цим документи;

d) документи, зокрема протоколи, які є вимогою цього стандарту;

e) визначені організацію документи, зокрема протоколи, які необхідні для забезпечення результативних процесів планування, функціювання та контролювання, пов'язаних зі значними загрозами безпеці та ризиками.

Організація повинна визначити ступінь конфіденційності інформації стосовно безпеки та вжити заходів для запобігання несанкційованому доступу до неї.

4.4.5 ***Контроль документів і даних***

Організація повинна розробити та підтримувати методики контролювання всіх документів, даних та інформації, які є вимогою розділу 4 цього стандарту, для забезпечення того, щоб

a) лише уповноважені працівники могли зберігати ці документи, дані й інформацію та мали доступ до них;

b) уповноважений персонал періодично аналізував та, за потреби, переглядав і затверджував ці документи, дані й інформацію щодо їх відповідності;

c) чинні версії відповідних документів, даних та інформації були наявними на всіх місцях, де виконують роботи, важливі для результативного функціювання системи управління безпекою;

d) застарілі документи, дані та інформацію відразу було вилучено з усіх місць видавання та місць використовування, або іншим способом захищено від ненавмисного використовування;

e) документи, дані та інформація, що їх зберігають в архіві як юридичний доказ або джерело знань, або як перше та друге, було належним чином позначено;

f) ці документи, дані та інформацію було захищено, а в разі їх наявності в електронному вигляді, щоб вони мали належні резервні копії й уможливлювали їх відновлення.

4.4.6 ***Операційний контроль***

Організація повинна визначити роботи та дії, необхідні для

a) реалізації своєї політики у сфері управління безпекою;

b) контролювання робіт і лом'якшування загроз, що мають значний ступінь ризику;

c) досягнення відповідності правовим, статутним та іншим нормативним вимогам у сфері безпеки;

d) досягнення своїх цілей у сфері управління безпекою;

e) забезпечування формування своїх програм щодо управління безпекою;

f) досягнення необхідного рівня безпеки ланцюга постачання.

Організація повинна забезпечувати, щоб ці роботи та дії виконували за встановлених умов, через

a) розроблляння, запроваджування та підтримування задокументованих методик контролювання ситуацій, якщо їх відсутність може призводити до неспроможності виконання дій і робіт, перелічених вище у 4.4.6 a) — f);

b) оцінювання будь-яких загроз, пов'язаних з видами робіт у ланцюзі постачання на висхідному потоці, і застосовування заходів контролю, щоб пом'якшувати ці впливи на організацію та інші сторони у ланцюзі постачання на низхідному потоці;

c) установлення та дотримання вимог до виробів і послуг, які впливають на безпеку, та інформування про них постачальників і підрядників.

Потрібно, щоб методики охоплювали заходи контролювання щодо проектування, встановлення, функціювання, відновлення та зміни одиниць устаткування, апаратури тощо, пов'язаних з безпекою, як належить. У разі перегляду наявних заходів або введення нових заходів, які можуть впливати на роботи та дії щодо управління безпекою, організація повинна розглянути пов'язані з ними загрози безпеці та ризики перед їх реалізацією. Потрібно, щоб нові чи переглянуті заходи, які підлягають розгляду, охоплювали

a) переглянуті організаційну структуру, функції чи відповідальність;

b) переглянуті політику, цілі, завдання чи програми у сфері управління безпекою;

c) переглянуті процеси чи методики;

d) запроваджування нових інфраструктур, пов'язаних з безпекою устаткування чи технологій, які можуть охоплювати технічні та/або програмні засоби;

e) залучення нових підрядників, постачальників чи нового персоналу, за обставинами.

4.4.7 ***Готовність до надзвичайних ситуацій, реагування на них і відновлення безпеки***

Організація повинна розробити, запровадити та підтримувати прийнятні плани і методики визначання можливих аварій і надзвичайних ситуацій, пов'язаних з безпекою, та реагування на них, а також запобігання та пом'якшення ймовірних наслідків, які може бути пов'язано з ними. Потрібно, щоб у планах та методиках була інформація про надання й підтримання будь-якого ідентифікованого устаткування, ідентифікованих виробничих об'єктів чи послуг, що їх можуть вимагати під час або після аварій чи надзвичайних ситуацій.

Організація повинна періодично аналізувати результативність своїх планів і методик щодо готовності до надзвичайних ситуацій, реагування на них і відновлення безпеки, зокрема після виникнення аварій чи надзвичайних ситуацій, спричинених порушеннями та загрозами безпеці. Організація повинна періодично апробовувати ці методики, якщо це практично можливо.

4.5 Перевіряння та коригувальні дії

4.5.1 ***Вимірювання та моніторинг дієвості у сфері безпеки***

Організація повинна розробити та підтримувати методики моніторингу та вимірювання дієвості своєї системи управління безпекою. Вона повинна також розробити та підтримувати методики моніторингу та вимірювання дієвості у сфері безпеки. Установлюючи частоту проведення вимірювань і моніторингу основних параметрів діяльності, організація повинна розглянути пов'язані загрози безпеці та ризики, зокрема потенційні механізми погіршення та їхні наслідки. Потрібно, щоб у цих методиках було передбачено

a) як якісні, так і кількісні вимірювання, що відповідають потребам організації;

b) моніторинг ступеня, у який дотримують політику, досягають цілі та виконують завдання організації у сфері управління безпекою;

c) випереджувальні (проактивні) заходи, щоб здійснювати моніторинг відповідності програмам управління безпекою, критеріям операційного контролю та застосовним правовим, статутним та іншим нормативним вимогам у сфері безпеки;

d) виправні (реактивні) заходи для проведення моніторингу пов'язаних з безпекою погіршень, відмов, інцидентів, невідповідностей (зокрема відсутність і хибність сигналів тривоги) та інших фактів недостатньої дієвості системи управління безпекою;

e) реєстрування даних і результатів моніторингу та вимірювання, достатніх для полегшення подальшого аналізування коригувальних і запобіжних дій. Якщо для забезпечення дієвості та/або вимірювання й моніторингу потрібне устаткування для моніторингу, організація повинна вимагати розроблення та підтримування методик для калібрування й технічного обслуговування цього устаткування. Протоколи виконання та результатів калібрування й технічного обслуговування потрібно зберігати протягом достатнього часу відповідно до законодавства та політики організації.

4.5.2 ***Оцінювання системи***

Організація повинна оцінювати плани, методики та можливості у сфері управління безпекою за допомогою періодичних аналізувань, випробовувань, звітів про наслідки аварій, здобутих уроків, оцінювань дієвості та вправ. Значні зміни у цих чинниках потрібно негайно відображати в методиках.

Організація повинна періодично оцінювати дотримання відповідного законодавства та регламентів, найкращої промислової практики, а також відповідність своїм власним політиці та цілям.

Організація повинна вести протоколи результатів періодичних оцінювань.

4.5.3 ***Відмови, аварії, невідповідності, коригувальні та запобіжні дії, пов'язані з безпекою***

Організація повинна розробити, запровадити та підтримувати методики визначання відповідальності та повноважень для

a) оцінювання та ініціювання запобіжних дій для ідентифікування потенційних відмов безпеки з тим, щоб можна було запобігати їх виникненню;

b) розслідувань, пов'язаних з безпекою

1) відмов, зокрема відсутності та хибності сигналів тривоги;

2) аварій і надзвичайних ситуацій;

3) невідповідностей;

c) виконання дій для пом'якшення будь-яких наслідків цих відмов, аварій чи невідповідностей;

d) ініціювання та виконання коригувальних дій;

e) підтвердження результативності виконаних коригувальних дій.

Потрібно, щоб у цих методиках було встановлено вимогу стосовно того, щоб усі запропоновані коригувальні та запобіжні дії аналізували в межах процесу загального оцінювання загроз безпеці та ризиків перед їх виконанням, крім випадків, коли негайне виконання перешкоджає неминучим впливам на здоров'я чи суспільну безпеку.

Потрібно, щоб будь-які коригувальні чи запобіжні дії, виконувані для усунення причин фактичних і потенційних невідповідностей, відповідали важливості проблем та були сумірними з тими загрозами та ризиками, пов'язаними з управлінням безпекою, які можуть виникнути. Організація повинна реалізовувати та реєструвати будь-які зміни у задокументованих методиках, які є результатом коригувальних і запобіжних дій, і, якщо необхідно, повинна забезпечувати потрібне навчання персоналу.

4.5.4 ***Контроль протоколів***

Організація повинна розробити та вести протоколи, необхідні, щоб показати відповідність вимогам своєї системи управління безпекою та цього стандарту, а також показати досягнені результати.

Організація повинна розробити, запровадити та підтримувати методику щодо позначання, накопичування, захисту, пошуку, зберігання та вилучення протоколів.

Потрібно, щоб протоколи завжди були розбірливими, придатними для розпізнавання та простежування.

Електронна та цифрова документація має бути захищена від копіювання, надійно зарезервована та доступна тільки для уповноваженого персоналу.

4.5.5 ***Аудит***

Організація повинна розробити, запровадити та підтримувати програму аудиту управління безпекою та повинна забезпечувати проведення аудитів системи управління безпекою у заплановані проміжки часу, для того щоб

a) визначати, чи система управління безпекою

1) відповідає запланованим заходам щодо управління безпекою, зокрема вимогам усього розділу 4 цього стандарту;

2) належним чином запроваджена та підтримувана;

3) є результативною щодо задоволення політики та досягнення цілей організації у сфері управління безпекою;

b) аналізувати результати попередніх аудитів і дії, виконані для виправлення невідповідностей;

c) подавати керівництву інформацію про результати аудитів;

d) перевіряти, чи належним чином задіяно устаткування та персонал, пов'язані з безпекою.

Потрібно, щоб основою програми аудиту, зокрема будь-якого графіка, були результати загального оцінювання загроз і ризиків діяльності організації та результати попередніх аудитів. Потрібно, щоб у методиках аудиту було описано сферу застосування, періодичність, методології та компетентність, а також відповідальність і вимоги щодо проведення аудитів і звітування про результати. Де можливо, аудити повинен провадити персонал, незалежний від тих, хто безпосередньо відповідає за діяльність, яку перевіряють.

Примітка. Фраза «незалежний персонал» не обов'язково означає сторонній щодо організації персонал.

4.6 Аналізування з боку керівництва та постійне поліпшування

Найвище керівництво повинне із запланованою періодичністю аналізувати систему управління безпекою організації, щоб забезпечувати її постійну придатність, адекватність і результативність. Потрібно, щоб аналізування охоплювало загальне оцінювання можливостей щодо поліпшування та потребу в змінах до системи управління безпекою, а також політику, цілі, загрози та ризики, пов'язані з безпекою. Потрібно вести протоколи аналізування з боку керівництва. Потрібно, щоб до вхідних даних аналізування з боку керівництва належали

a) результати аудитів і оцінювань дотримання відповідності правовим вимогам та іншим вимогам, які організація зобов'язується виконувати;

b) інформація від зовнішніх зацікавлених сторін, зокрема скарги;

c) дієвість організації щодо безпеки;

d) досягнення цілей і виконання завдань;

e) статус коригувальних і запобіжних дій;

f) дії за результатами попереднього аналізування з боку керівництва;

g) змінення обставин, зокрема зміни в правових та інших вимогах, пов'язаних з аспектами безпеки;

h) рекомендації щодо поліпшування.

Потрібно, щоб результатами аналізування з боку керівництва були рішення та дії, пов'язані з можливими змінами в політиці, цілях, завданнях у сфері управління безпекою, а також інших елементах системи управління безпекою відповідно до зобов'язання організації щодо постійного поліпшування.

ДОДАТОК А
(довідковий)

ВІДПОВІДНІСТЬ МІЖ ISO 28000:2007, ISO 14001:2004 ТА ISO 9001:2000

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Вимоги до системи управління безпекою ланцюга постачання (лише заголовок)	4	Вимоги до системи екологічного управління (лише заголовок)	4	Вимоги до системи управління якістю (лише заголовок)	4
Загальні вимоги	4.1	Загальні вимоги	4.1	Загальні вимоги	4.1
Політика у сфері управління безпекою	4.2	Екологічна політика	4.2	Зобов'язання керівництва	5.1
				Політика у сфері якості	5.3
				Постійне поліпшування	8.5.1
Загальне оцінювання та планування ризиків (лише заголовок)	4.3	Планування (лише заголовок)	4.3	Планування (лише заголовок)	5.4
Загальне оцінювання ризиків	4.3.1	Екологічні аспекти	4.3.1	Орієнтація на замовника	5.2
				Визначання вимог щодо продукції	7.2.1
				Аналізування вимог щодо продукції	7.2.2

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Правові, статутні та інші нормативні вимоги у сфері безпеки	4.3.2	Правові та інші вимоги	4.3.2	Орієнтація на замовника	5.2
				Визначання вимог щодо продукції	7.2.1
Цілі у сфері управління безпекою	4.3.3	Цілі, завдання та програми	4.3.3	Цілі у сфері якості	5.4.1
				Планування системи управління якістю	5.4.2
				Постійне поліпшування	8.5.1
Завдання у сфері управління безпекою	4.3.4	Цілі, завдання та програми	4.3.3	Цілі у сфері якості	5.4.1
				Планування системи управління якістю	5.4.2
				Постійне поліпшування	8.5.1
Програми у сфері управління безпекою	4.3.5	Цілі, завдання та програми	4.3.3	Цілі у сфері якості	5.4.1
				Планування системи управління якістю	5.4.2
				Постійне поліпшування	8.5.1
Запроваджування та функціювання (лише заголовок)	4.4	Запроваджування та функціювання (лише заголовок)	4.4	Виготовляння продукції (лише заголовок)	7
Структура, повноваження та відповідальність щодо управління безпекою	4.4.1	Ресурси, функційні обов'язки, відповідальність і повноваження	4.4.1	Зобов'язання керівництва	5.1
				Відповідальність і повноваження	5.5.1
				Представник керівництва	5.5.2
				Забезпечення ресурсами	6.1
				Інфраструктура	6.3
Компетентність, підготовленість і обізнаність	4.4.2	Компетентність, підготовленість і обізнаність	4.4.2	(Людські ресурси) Загальні положення	6.2.1
				Компетентність, обізнаність і підготовленість	6.2.2
Обмін інформацією	4.4.3	Інформування	4.4.3	Внутрішнє інформування	5.5.3
				Інформаційний зв'язок із замовниками	7.2.3
Документація	4.4.4	Документація	4.4.4	(Вимоги до документації) Загальні положення	4.2.1
Контроль документів і даних	4.4.5	Контроль документів	4.4.5	Контроль документів	4.2.3
Операційний контроль	4.4.6	Операційний контроль	4.4.6	Планування виготовляння продукції	7.1
				Визначання вимог щодо продукції	7.2.1
				Аналізування вимог щодо продукції	7.2.2
				Планування проектування та розробляння	7.3.1
				Вхідні дані проектування та розробляння	7.3.2
				Вихідні дані проектування та розробляння	7.3.3

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
				Аналізування проекту та розробки	7.3.4
				Перевіряння проекту та розробки	7.3.5
				Затверджування проекту та розробки	7.3.6
				Контроль змін у проекті та розробці	7.3.7
				Процес закупівлі	7.4.1
				Інформація стосовно закупівлі	7.4.2
				Перевіряння закупленої продукції	7.4.3
				Контроль виробництва та обслуговування	7.5.1
				Затверджування процесів виробництва та обслуговування	7.5.2
				Зберігання продукції	7.5.5
Готовність до надзвичайних ситуацій, реагування на них і відновлення безпеки	4.4.7	Готовність до надзвичайних ситуацій і реагування на них	4.4.7	Контроль невідповідної продукції	8.3
Перевіряння та коригувальні дії (лише заголовок)	4.5	Перевіряння (лише заголовок)	4.5	Вимірювання, аналізування та поліпшування (лише заголовок)	8
Вимірювання та моніторинг дієвості у сфері безпеки	4.5.1	Моніторинг і вимірювання	4.5.1	Контроль засобів моніторингу та вимірювання	7.6
				Загальні положення (вимірювання, аналіз і поліпшування)	8.1
				Моніторинг і вимірювання процесів	8.2.3
				Моніторинг і вимірювання продукції	8.2.4
				Аналізування даних	8.4
Оцінювання системи	4.5.2	Оцінювання дотримання відповідності	4.5.2	Моніторинг і вимірювання процесів	8.2.3
				Моніторинг і вимірювання продукції	8.2.4
Відмови, аварії, невідповідності, коригувальні та запобіжні дії, пов'язані з безпекою	4.5.3	Невідповідність, коригувальні та запобіжні дії	4.5.3	Контроль невідповідної продукції	8.3
				Аналізування даних	8.4
				Коригувальні дії	8.5.2
				Запобіжні дії	8.5.3
Контроль протоколів	4.5.4	Контроль протоколів	4.5.4	Контроль протоколів	4.2.4
Аудит	4.5.5	Внутрішній аудит	4.5.5	Внутрішній аудит	8.2.2
Аналізування з боку керівництва та постійне поліпшування	4.6	Аналізування з боку керівництва	4.6	Зобов'язання керівництва	5.1
				Аналізування з боку керівництва (лише заголовок)	5.6
				Загальні положення	5.6.1
				Вхідні дані аналізування	5.6.2
				Результати аналізування	5.6.3
				Постійне поліпшування	8.5.1

БІБЛІОГРАФІЯ

1 ISO 9001:2000 Quality management systems — Requirements

2 ISO 14001:2004 Environmental management systems — Requirements with guidance for use

3 ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing

4 ISO/PAS 20858:2004 Ships and marine technology — Maritime port facility security assessments and security plan development

5 ISO/PAS 28001 Security management systems for the supply chain — Best practices for implementing supply chain security — Assessments and plans

6 ISO/PAS 28004:2006 Security management systems for the supply chain — Guidelines for the implementation of ISO/PAS 28000

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

1 ISO 9001:2000 Системи управління якістю. Вимоги[1)]

2 ISO 14001:2004 Системи екологічного управління. Вимоги та настанови щодо застосовування[2)]

3 ISO 19011:2002 Настанови щодо здійснення аудитів систем управління якістю і (або) екологічного управління[3)]

4 ISO/PAS 20858:2004 Судна та технологія морських робіт. Оцінювання безпеки споруд морських портів і розроблляння плану безпеки[4)]

5 ISO/PAS 28001 Системи управління безпекою ланцюга постачання. Найкращі методи запроваджування безпеки ланцюга постачання. Оцінки та плани[5)]

6 ISO/PAS 28004:2006 Системи управління безпекою ланцюга постачання. Настанови щодо запроваджування ISO/PAS 28000[6)].

[1)] Стандарт ISO 9001:2000 впроваджено в Україні як ДСТУ ISO 9001-2001 Системи управління якістю. Вимоги

[2)] Стандарт ISO 14001:2004 впроваджено в Україні як ДСТУ ISO 14001:2006 Системи екологічного керування. Вимоги та настанови щодо застосовування

[3)] Стандарт ISO 19011:2002 впроваджено в Україні як ДСТУ ISO 19011:2003 Настанови щодо здійснення аудитів систем управління якістю і (або) екологічного управління

[4)] На заміну ISO/PAS 20858 опубліковано стандарт ISO 20858:2007 *Ships and marine technology — Maritime port facility security essessments and security plan development*, який не впроваджено в Україні як національний і чинного документа на цей об'єкт стандартизації немає

[5)] На заміну ISO/PAS 28001 опубліковано стандарт ISO 28001:2007 *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance*, який не впроваджено в Україні як національний і чинного документа на цей об'єкт стандартизації немає

[6)] На заміну ISO/PAS 28004 опубліковано стандарт ISO 28004:2007 *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000*, який не впроваджено в Україні як національний і чинного документа на цей об'єкт стандартизації немає.

Код УКНД 47.020.99

Ключові слова: безпека, зацікавлена сторона, ланцюг постачання, постійне поліпшування, система управління безпекою, управління безпекою.

Редактор **Н. Куземська**
Технічний редактор **О. Касіч**
Коректор **О. Рождественська**
Верстальник **Т. Шишкіна**

Підписано до друку 07.02.2011. Формат 60 × 84 1/8.
Ум. друк. арк. 2,32. Обл.-вид. арк. 1,46. Зам. 239 Ціна договірна.

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

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