УДК 004.056.5

Цвілій О. О., аспірантка
(Одеська національна академія зв'язку ім. О. С. Попова, +380 67 248 05 59, o.tsviliy@ukr.net)

БЕЗПЕКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: СУЧАСНИЙ СТАН СТАНДАРТІВ ISO27k СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Цвілій О. О. Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою. У статті досліджено сучасний стан та напрямки розвитку стандартів ISO27k систем управління інформаційною безпекою (СУІБ). Зроблено систематизований огляд версій основних стандартів СУІБ. Показано місце та роль цих стандартів в системі оцінки відповідності України. Розглянуті питання гармонізації нормативно-правового забезпечення України щодо оцінки відповідності СУІБ за правилами та процедурами згідно міжнародних стандартів.

Ключові слова: система управління, інформаційна безпека, стандарти ISO27k, органи оцінки відповідності, сертифікація, акредитація

Цвилий Е. А. Безопасность информационных технологий: современное состояние стандартов ISO27k систем менеджмента информационной безопасности. В статье исследовано современное состояние и направления развития стандартов ISO27k систем менеджмента информационной безопасности (СМИБ). Сделано систематизированный обзор версий основных стандартов СМИБ. Показано место и роль этих стандартов в системе оценки соответствия Украины. Рассмотрены вопросы гармонизации нормативно правового обеспечения Украины относительно оценки соответствия СМИБ за правилами и процедурами согласно международных стандартов.

***Ключевые слова*:** система менеджмента, информационная безопасность, стандарты ISO27k, органы оценки соответствия, сертификация, аккредитация

Tsviliy O. O. IT security techniques: current state ISO27k standards of information security management system. The current state and direction of ISO27k standards for information security management systems (ISMS) is investigated. A systematic review of all major versions of ISMS standards is made. The place and role of ISO27k standards for conformity assessment systems in Ukraine is shown. The questions of harmonization normatively of the legal providing of Ukraine are considered in relation to the estimation of accordance of ISMS after rules and procedures in obedience to international standards.

Keywords: management system, information security, ISO27k standards, conformity assessment bodies, certification, accreditation

1. Вступ і постановка задачі. Вся інформація, що зберігається і обробляється у організації, є об'єктом погроз атаки, помилки, впливу стихії (наприклад, повені або пожежі) і т.д. Термін «інформаційна безпека» відноситься до інформації, яку розглядають як актив, у якого є цінність, що вимагає відповідного захисту, наприклад, від втрати доступності, конфіденційності чи цілісності [1].

Захист інформаційних активів за допомогою створення, впровадження, підтримки і поліпшення інформаційної безпеки дуже важливий для того, щоб дозволити організації досягати своєї цілі, а також підтримувати і підвищувати рівень відповідності законодавству та репутацію. Ці скоординовані дії, які направляють реалізацію відповідних засобів управління та розглядають неприпустимі ризики інформаційної безпеки, є загальновідомими як елементи системи управління інформаційною безпекою (СУІБ), яка є частиною загальної системи управління організації.

Міжнародні організації доклали великих зусиль для уніфікації СУІБ. В повній мірі це досягнуто в серії міжнародних стандартів СУІБ. Дане сімейство має схему нумерації, що використовує серію послідовних номерів, починаючи з 27000 – стандарти ISO27k [2]. Стандарти цього сімейства визначають вимоги до СУІБ, управління ризиками, метрики і вимірювання, керівництво з впровадження тощо.

При використанні стандартів ISO27k організації можуть реалізовувати і поліпшувати СУІБ та підготуватися до незалежної оцінки їх СУІБ в органах оцінки відповідності (ООВ), які є акредитованими та визнаними в міжнародній системі акредитації International Accreditation Forum (IAF), наприклад, Європейською асоціацією з акредитації (ЄА). Далі під СУІБ будемо розуміти саме таку систему, яка створена у відповідності до вимог стандартів серії ISO27k.

Сімейство міжнародних стандартів СУІБ ISO27k розробляє Об'єднаний технічний комітет ISO/IEC JTC 1, підкомітет SC 27 «Методи захисту ІТ» (ISO/IEC JTC 1/SC 27 «Методи і засоби забезпечення безпеки інформаційних технологій» (англ.: – IT Security techniques)) [3]. Загальна кількість опублікованих стандартів ISO під прямою відповідальністю ISO/IEC JTC 1/SC 27 – 137, в тому числі стандартів ISO27k – 28.

Стандарти ISO27k можуть бути класифіковані за рівнями ієрархії, як відображено на Рис. 1 [1]. При цьому перші три рівні ієрархії можемо об’єднати поняттям системостворюючих стандартів або стандартів вищих рівнів. Всі інші стандарти ISO27k, які знаходяться на четвертому і, можливо, нижчих рівнях, об’єднаємо поняттям стандартів прикладних рівнів.

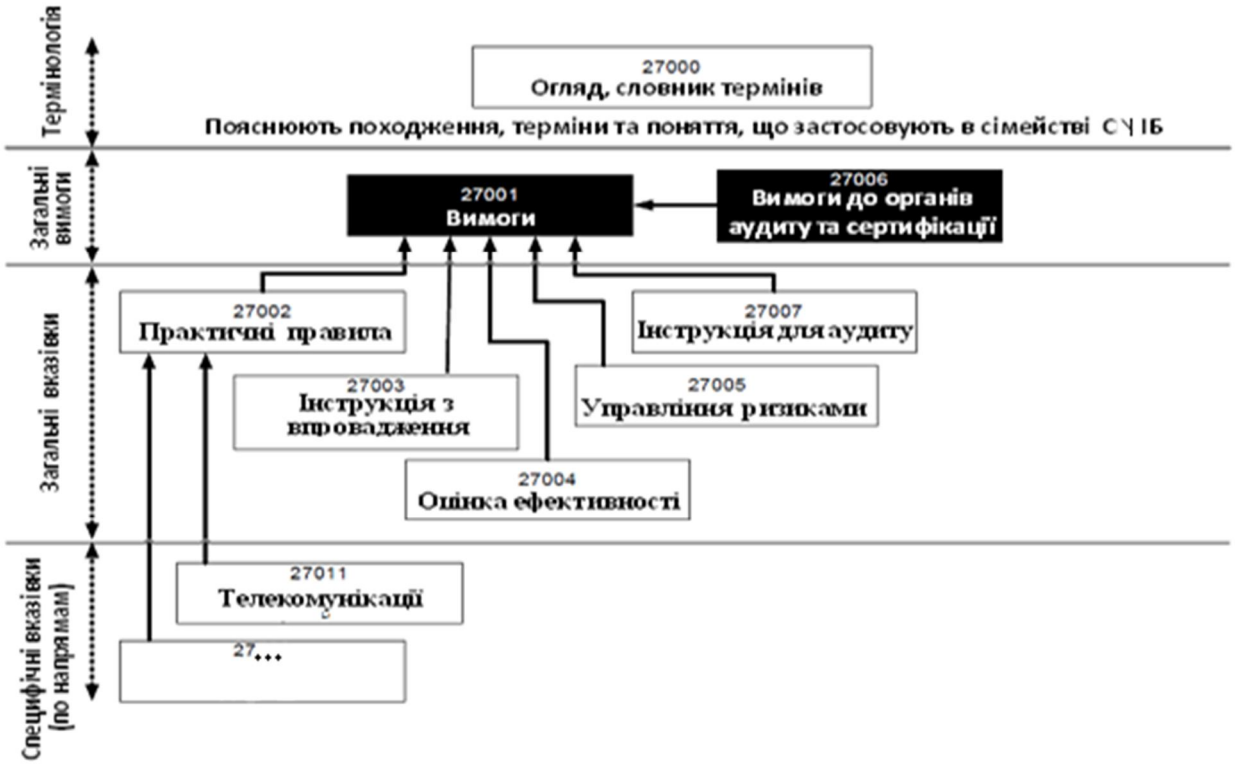

Рис. 1. Ієрархія стандартів СУІБ (ISMS – Information Security management systems)

В статті надається стислий систематизований огляд актуальних стандартів вищих трьох рівнів стандартів ISO27k. Саме ці рівні ієрархії стандартів ISO27k надають можливість застосовувати до СУІБ процедури оцінки відповідності (сертифікації) систем управління ООВ, компетентність яких прослідковується та визнається на глобальному рівні в міжнародній системі акредитації IAF. Саме тому, в статті стисло відображена національна система України, яка дозволяє здійснювати процедури оцінки відповідності (сертифікації) СУІБ таким чином, що результати таких оцінок можуть бути визнаними згідно кращих міжнародних практик.

2. Огляд стандартів ISO27k вищих рівнів. Стандарти ISO27k вищих рівнів під загальною назвою «Інформаційні технології. Методи і засоби забезпечення безпеки» (англ. Information technology. Security techniques) складаються з наступних груп: термінологія; загальні вимоги; загальні вказівки (Рис. 1).

ISO/IEC 27000:2014 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд та словник» (англ.: Information technology – Security techniques – Information security management systems – Overview and vocabulary) – описує огляд та словник СУІБ, які є предметом стандартів ISO27k, і визначає відповідні терміни та визначення [3].

Для того, щоб відобразити стан змін стандартів ISO27k, цей стандарт оновлюється частіше, ніж зазвичай оновлюються стандарти ISO/IEC. Попередня редакція цього стандарту є ISO/IEC 27000:2012.

ISO/IEC 27001:2013 «Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи управління інформаційною безпекою. Вимоги» (англ.: Information technology – Security techniques. Information security management systems – Requirements). Цей стандарт є базовим стандартом ISO27k.

ISO/IEC 27001 визначає вимоги для створення, впровадження, експлуатації, моніторингу, аналізу, підтримки і поліпшення документованої СУІБ в контексті загальних ризиків організації бізнесу. Цей стандарт призначений для забезпечення вибору адекватного і пропорційного контролю систем інформаційної безпеки.

Стандарт ISO/IEC 27001 призначений для сертифікації СУІБ в ООВ. В Україні ООВ, який здійснює сертифікацію СУІБ, з можливістю визнання сертифікату за межами країни повинен бути акредитованим національним органом з акредитації, яким з 2002 року є Національне агентство з акредитації України (НААУ) і якому надані державні ексклюзивні повноваження на акредитацію ООВ та проведення моніторингу за відповідністю акредитованих ним ООВ вимогам акредитації [4].

На сьогодні в реєстрі НААУ вже є ООВ, акредитовані згідно стандарту ISO/IEC 17021:2011 «Оцінка відповідності. Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту (англ.: Conformity assessment – Requirements for bodies providing audit and certification of management systems) щодо компетентності здійснювати сертифікацію СУІБ відповідно до стандарту ISO/IEC 27001.

Сертифікована СУІБ – гарантія того, що СУІБ правильно і ефективно впроваджена в область (області) діяльності організації. А ефективна СУІБ, у свою чергу, забезпечує необхідний рівень захисту активів організації, тобто істотно знижує ризик нанесення

організації збитку внаслідок порушення інформаційної безпеки і гарантує, що міри і кошти захисту інформації є адекватному і пропорційними можливому збитку організації.

Сертифікація на відповідність цього стандарту дозволяє наочно показати діловим партнерам, інвесторам і клієнтам, що у організації налагоджене ефективне управління інформаційною безпекою.

Виконання вимог стандарту ISO/IEC 27001 головним чином дозволяє мінімізувати ризики втрат активів організацій, а отже скоротити фінансові втрати.

Відповідно до цього стандарту система управління інформаційною безпекою ISMS (англ.: Information security management system) – це частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, аналізу, підтримування та поліпшення інформаційної безпеки [5].

Важливо наголосити, що стандарт ISO/IEC 27001 системно та структурно узгоджено із стандартами ISO 9001:2000 та ISO 14001:2004 з метою підтримки послідовного та комплексного впровадження і функціонування разом з іншими пов'язаними стандартами загальних систем управління. Таким чином, одна, відповідним чином запроектована система управління, може задовольняти вимогам всіх цих стандартів. Тобто, цей стандарт розроблено для надання можливості організації узгодити свою СУІБ з відповідними вимогами загальної системи управління або інтегрувати її в них. Якщо організація вже має функціонуючу систему управління бізнес-процесами (наприклад, відповідно до ISO 9001 або ISO 14001), то в більшості випадків краще задовольнити вимоги цього стандарту в межах цієї існуючої системи управління.

В Україні у 2012 році вступив дію стандарт ДСТУ ISO/IEC 27001:2010, затверджений наказом Держспоживстандарту від 28 грудня 2010 р. № 631, який відповідає попередній редакції міжнародного стандарту ISO/IEC 27001:2005, IDT.

ISO/IEC 27002:2013 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою» (англ.: Information technology – Security techniques – Code of practice for information security management).

ISO/IEC 27002 встановлює принципи і загальні принципи розробки, впровадження, підтримки і поліпшення управління інформаційною безпекою в організації. Цілі, викладені в стандарті, дозволяють забезпечити загальне керівництво за загальноприйнятою мети управління інформаційною безпекою.

Відповідно до цього стандарту інформаційна безпека – це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес ризику і максимізації рентабельності інвестицій і бізнес можливостей [6].

Інформаційна безпека досягається впровадженням відповідного набору управлінських заходів (далі – заходів), який охоплює політику, процеси, процедури, організаційні структури і програмні та апаратні функції. Ці заходи необхідно розробити, впровадити, моніторити, переглядати та, за необхідності, вдосконалювати для гарантування того, що певні безпека та бізнес-цілі організації будуть досягнуті. Це треба виконувати узгоджено з іншими процесами загального управління бізнесом.

В стандарті викладено детальний звід правил для управління інформаційною безпекою.

Попередня редакція цього стандарту є ISO/IEC 27002:2005.

ISO/IEC 27003:2010 «Інформаційні технології. Методи захисту. Керівництво по впровадженню системи управління інформаційною безпекою» (англ.: Information technology – Security techniques – Information security management system implementation guidance).

ISO/IEC 27003 фокусується на критичних аспектах, необхідних для успішної розробки і впровадженню СУІБ відповідно до ISO/IEC 27001. Стандарт описує процес специфікації і розробки СУІБ від початку до впровадження планів реалізації.

Цей стандарт описує процес отримання схвалення керівництва для реалізації СУІБ, визначає порядок проектування і впровадження СУІБ (посилання в ISO/IEC 27003 в якості проекту СУІБ) і дає рекомендації про те, як планувати проект СУІБ, в результаті чого остаточна СУІБ стає планом реалізації проекту.

В стадії розробки знаходиться друга редакція цього стандарту (ISO/IEC WD 27003).

ISO/IEC 27004:2009 «Інформаційні технології. Методи забезпечення безпеки. Керівництво інформаційною безпекою. Вимірювання» (англ.: Information technology – Security techniques – Information security management – Measurement).

ISO/IEC 27004 являє собою керівництво з розробки та впровадження заходів з вимірювань в цілях оцінки ефективності реалізації СУІБ і управління або групи елементів управління, як зазначено в ISO/IEC 27001.

В стадії розробки знаходиться друга редакція цього стандарту (ISO/IEC WD 27004).

ISO/IEC 27005:2011 «Інформаційні технології. Методи забезпечення безпеки. Керівництво ризиками інформаційної безпеки» (англ.: Information technology – Security techniques – Information security risk management).

Стандарт ISO/IEC 27005 вийшов на заміну стандарту ISO/IEC 27005:2008. В стадії розробки знаходиться третя редакція цього стандарту (ISO/IEC WD 27005).

ISO/IEC 27005 – нова версія стандарту з управління ризиками інформаційної безпеки вже опублікована і доступна для зацікавлених сторін. Стандарт є відмінним інструментом для успішного вирішення однієї з найскладніших завдань у впровадженні та розвитку СУІБ – оцінка та керівництво ризиками інформаційної безпеки.

Основні зміни в новій версії стандарту пов'язані з його гармонізацією з стандартом ISO 31000:2009 «Управління ризиками. Принципи і керівні вказівки» (англ.: Management du risque – Principes et lignes directrices) і з кращою систематизацією змісту.

ISO/IEC 27006:2011 «Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою» (англ. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems).

Стандарт ISO/IEC 27006 вийшов на заміну стандарту ISO/IEC 27006:2007 та ефективно замінює ЕА 7/03 «Керівництво з акредитації органів з сертифікації/реєстрації. Системи управління інформаційною безпекою» (англ.: Guidelines for the Accreditation of bodies operating certification/registration – Information Security Management Systems).

В умовах діючої національної системи акредитації України (яка відповідає вимогам стандарту ISO/IEC 17011:2004 «Оцінювання відповідності. Загальні вимоги до органів акредитації, що акредитують органи оцінювання відповідності» (англ.: – Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment

bodies)) стандарт ISO/IEC 27006 формує вимоги до органів аудиту і сертифікації СУІБ, які можуть бути акредитовані на відповідність вимогам стандарту ISO/IEC 17021.

В стадії розробки знаходиться третя редакція цього стандарту (ISO/IEC CD 27006).

ISO/IEC 27007:2011 «Інформаційні технології. Методи забезпечення безпеки. Керівництво для аудиту систем управління інформаційною безпекою» (англ.: Information technology – Security techniques – Guidelines for information security management systems auditing).

Стандарт ISO/IEC 27007 являє собою посібник з створення в СУІБ програм аудиту з проведення аудитів, а також щодо компетентності аудиторів СУІБ (крім вказівок, що містяться в стандарті ДСТУ ISO 19011:2012 «Настанови щодо здійснення аудитів систем управління» (англ.: Guidelines for auditing management systems, ISO 19011:2011, IDT).

Тобто, стандарт ISO/IEC 27007 застосуємо у разі необхідності проведення внутрішніх чи зовнішніх аудитів СУІБ або створення програми аудиту СУІБ.

3. Гармонізація нормативно-правового забезпечення України щодо оцінки віповідності СУІБ за правилами та процедурами згідно міжнародних стандартів. В Україні створена та діє система, яка дозволяє здійснювати процедури оцінки відповідності (сертифікації) СУІБ таким чином, що результати таких оцінок можуть бути визнаними згідно кращих міжнародних практик. Це створює передумови для усунення технічних бар'єрів між країнами в сфері технічного регулювання, в тому числі з питань систем управління (поряд з оцінкою відповідності продукції, послуг, процесів тощо). Такі засади є обов'язковими для країн – підписантів багатьох міжнародних договорів, в тому числі Угоди про технічні бар'єри в торгівлі та Угоди про застосування санітарних і фітосанітарних заходів з Світовою організацією торгівлі (СОТ) (англ.: World Trade Organization, WTO), майбутньої Угоди про асоціацію України з Європейським Союзом (ЄС), тощо.

До цієї системи входять.

1) Нормативно-правове забезпечення (закони України, національні стандарти та інші). Для проблематики питань, що розглядаються в статті, важливими є закон України «Про акредитацію органів з оцінки відповідності» від 17 травня 2001 року N 2407-III (із змінами і доповненнями 2012 року), стандарти ДСТУ ISO/IEC 17011:2005 (ISO/IEC 17011:2004, IDT), ISO/IEC 17021 (неофіційний переклад ISO/IEC 17021, Наказ НААУ від 11.09.2007 р. № 85-Я), ДСТУ ISO/IEC 27001 та інші.

2) Національна система акредитації України (НААУ), Рада з акредитації, Технічний комітет з акредитації, Комісія з апеляцій, Атестаційна комісія, експерти), яка має процедури і персонал з акредитації, які задовольняють вимогам стандарту ISO/IEC 17011:2004, IDT;

3) Органи з оцінки відповідності СУІБ, компетентність яких доведена шляхом акредитації в НААУ на відповідність вимогам стандарту ISO/IEC 17021 до органів, що здійснюють аудит і сертифікацію систем менеджменту, в сфері компетентності яких є оцінка відповідності вимогам стандарту ISO/IEC 27001.

4) Організації, які впроваджують СУІБ за вимогами та правилами міжнародних стандартів, що розглядаються вище, чи гармонізованими з ними національними стандартами. В даному випадку – ISO/IEC 27001.

Важливим елементом цієї системи є також визнання з боку однієї з регіональних асоціацій з акредитації НААУ на відповідність вимогам ISO/IEC 17011:2005. Всього в системі IAF налічується 6 таких асоціацій. Під час акредитації НААУ керується відповідними рекомендаціями міжнародних (ILAC та IAF) та регіональних (ЕА) організацій з акредитації. ЄА є інструментом співробітництва національно визнаних органів з акредитації в Європі. НААУ для сегменту систем управління (ISO/IEC 17021) має визнання з боку ЄА з 2012 року.

Таким чином, в Україні створена і функціонує національна система, яка дозволяє організаціям при використанні стандартів ISO27k реалізовувати і поліпшувати СУІБ та здійснювати її незалежну оцінку в органах оцінки відповідності (сертифікації), які є акредитованими та визнаними через визнання НААУ з боку ЕА в міжнародній системі акредитації IAF.

4. Результати, висновки, рекомендації. В статті викладено сучасний стан та напрямки розвитку версій стандартів ISO27k вищих рівнів систем управління інформаційною безпекою, достатніх для розробки, впровадження, аудиту та поліпшення СУІБ, які можуть бути оцінені (сертифіковані) за відповідними міжнародними правилами і процедурами, які прийняті на законодавчому та нормативно-правовому рівні в системі технічного регулювання, в тому числі оцінки відповідності та акредитації України.

Також, в загальному вигляді відображена національна система України, яка дозволяє здійснювати процедури оцінки відповідності (сертифікації) СУІБ таким чином, що результати таких оцінок можуть бути визнаними згідно кращих міжнародних практик.

В подальшому, в наступних публікаціях буде викладено сучасний стан та напрямки розвитку всіх версій стандартів ISO27k системи управління інформаційною безпекою прикладних рівнів, окремі аспекти щодо сертифікації СУІБ та акредитації ООВ, які є компетентними щодо сертифікації СУІБ.

Література

1. Information technology – Security techniques – Information security management systems - Overview and vocabulary // ISO/IEC 27000:2014 .

2. Information security standards [Електронний ресурс] // – Режим доступу : http://www.iso27001security.com (03.05.2014).

3. International Organization for Standardization [Електронний ресурс] // – Режим доступу : http://www.iso.org/iso/home.html (03.05.2014).

4. Національне агентство з акредитації України [Електронний ресурс] // – Режим доступу : http://naau.org.ua (04.05.2014).

5. Information technology – Security techniques – Information security management systems – Requirements // ISO/IEC 27001:2013.

6. Information technology – Security techniques – Code of practice for information security management // ISO/IEC 27002:2013.

Дата надходження в редакцію: 23.04.2014 р. Рецензент: д.т.н., проф. Горицький В. М.