# ТЕМА 4
# СТАНДАРТИЗАЦІЯ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 4.1 Вступ

Для розробки стандартів у галузі безпеки інформаційних технологій засновано підкомітет SC 27 “Security techniques” (Методи забезпечення безпеки) у рамках об’єднаного технічного комітету ISO/IEC JTC 1 "Information technology" (Інформаційні технології). Широкий спектр питань інформаційної безпеки, розглянутих фахівцями, залученими до діяльності SC 27, розподілений між п’ятьма робочими групами, що становлять весь підкомітет. За кожною групою закріплено відповідний напрям.

Перша робоча група (РГ 1) “Information Security Management Systems” (Системи менеджменту ІБ) займається розробкою стандартів і настановчих вказівок щодо побудови систем менеджменту інформаційної безпеки (ISMS).

Друга робоча група (РГ 2) “Cryptography and security mechanisms” (Шифрування і механізми безпеки) стосується стандартизації методів і механізмів забезпечення безпеки ІТ. .

Третя робоча група (РГ 3) “Security evaluation criteria” (Критерії оцінки безпеки) розробляє стандарти для оцінювання безпеки та сертифікації інформаційних систем та їх компонентів.

Четверта робоча група (РГ 4) “Security controls and services” (Контроль безпеки і послуг) займається розробкою і підтримкою стандартів і настановчих вказівок, що стосуються послуг і додатків, які сприяють реалізації заходів щодо захисту інформації, визначених у стандартах ISO/IEC 27001, 27002.

П’ята робоча група (РГ 5) “Identity management and privacy technologies” (Управління ідентифікаціями і конфіденційністю) розробляє стандарти та настановчі вказівки, що стосуються керування ідентифікаційними даними, біометрії та захисту персональних даних (privacy).

У своїй діяльності робочі групи дотримуються принципів і правил, прийнятим в ISO і IEC. Зокрема, у робочих групах повинні розроблятися і через кожні шість місяців переглядатися дорожні карти (road maps). Нижче ми зупинимося на змісті дорожньої карти, прийнятої в РГ 1.

Метою дорожньої карти є :

- точна ідентифікація стандартів, що стосуються РГ 1, як уже розроблених, так і розроблюваних або тих, що готуються до розробки;
- опис логічних зв'язків між розроблюваними в РГ 1 стандартами;
- створення підстав, за допомогою яких робота по створенню стандартів може бути скоординована для того, щоб уникнути непотрібного дублювання;
- можливість планування роботи з стандартизації в рамках РГ 1 в майбутньому;
- більша координація між різними технічними комітетами ISO і IEC.

### 4.2 Вимоги до стандартів, що розробляються

Стандарти, що розробляються в РГ1, стосуються захисту інформації, яка може існувати в різних видах (наприклад, бути надрукованою або написаною на папері, збереженою на електронних або магнітних носіях, переданою звичайною або електронною поштою, відеоінформацією, мовною інформацією). Також в РГ 1 розробляються стандарти, що стосуються механізмів, які обмежують шкоду, завдану організації через неналежний захист інформації (помилкові фінансові звіти, неправильні документи, випущені організацією, втрата репутації і престижу тощо).

Щоб ефективно вирішувати питання інформаційної безпеки, організації необхідно:

- систематично управляти діяльністю, пов'язаною з інформаційною безпекою;
- демонструвати свою здатність задовольнити вимоги внутрішніх і зовнішніх зацікавлених сторін.

Для того, щоб бути корисними різним організаціям, стандарти, які стосуються РГ1, повинні бути:

- згодженими (тобто мати спільну модель систем менеджменту, спільну структуру, узгоджену термінологію);
- взаємопов'язаними з іншими стандартами ISO, такими як ISO 9000 (серія стандартів з систем менеджменту якості), ISO 14000 (система стандартів з менеджменту навколишнього середовища).

Стандарти РГ1 повинні дотримуватись основних принципів, застосовуваних до стандартів з систем менеджменту, для того, щоб:

- допомогти користувачам реалізувати системи менеджменту;
- допомогти розробникам стандартів встановити узгоджену і логічну структуру.

### 4.3 Типи стандартів

Дорожня карта РГ1 дотримується чотирирівневої моделі, в рамках якої розробляються стандарти, які стосуються РГ1:

- тип А – термінологічний стандарт;
- тип В – стандарт, що стосується вимог;
- тип С – стандарт, що стосується надання настановчих вказівок (guidelines);
- тип D – суміжний стандарт.

Розглянемо ці типи більш детально.

*Тип А – термінологічний стандарт.*

Стандарт призначений для надання основної інформації, що включає загальну термінологію, яка узгоджено використовується у всій серії стандартів РГ1.

*Тип В – стандарт, що стосується вимог.*

Стандарт призначений для надання специфікацій, які відносяться до справи, що дозволяють організаціям демонструвати свою здатність задовольнити внутрішні та зовнішні вимоги з інформаційної безпеки.

Прикладами стандартів типу В є:

В–1: ISO/IEC 27001:2013. Системи менеджменту інформаційної безпеки – Вимоги.

В–2: ISO/IEC 27006:2015. Вимоги до органів, які проводять аудит і сертифікацію систем менеджменту інформаційної безпеки.

*Тип С – стандарт, що стосується надання настановчих вказівок.*

Стандарт призначений для допомоги організаціям у реалізації стандартів типу В.

Прикладами стандартів типу С є:

С-1:

- стандарти, що містять настанови щодо задоволення вимог до ISMS;
- стандарти, що містять настанови щодо вибору та реалізації заходів з інформаційної безпеки.

С-2:

- стандарти, що містять настанови щодо досягнення специфічних процесів, пов'язаних з менеджментом інформаційної безпеки (наприклад, вимірювання ефективності заходів);
- стандарти, що містять посібники з реалізації конкретних заходів/методів інформаційної безпеки (Менеджмент інцидентів інформаційної безпеки).

С-3:

- стандарти, що містять настанови щодо реалізації вимог з інформаційної безпеки, що враховують особливості галузі (банківська справа, розробка програмного забезпечення, охорона здоров'я, телекомунікації).

*Тип D – суміжний стандарт.*

Стандарт призначений для надання подальших настанов, що стосуються конкретних сторін інформаційної безпеки або суміжних методів підтримки. У загальному випадку, ці стандарти розробляються на односторонній основі без точних описів, що стосуються зв'язків зі стандартами типу В та/або типу С.

### 4.4 Елементи стандартів

Досвід, пов'язаний зі стандартами щодо систем менеджменту, які розробляються в ISO, показує, що в них існує ряд спільних елементів. Ці загальні елементи можна впорядкувати за такими основними темами:

- політика;
- планування;
- реалізація та експлуатація;
- оцінювання;

- покращення;
- перегляд керівництвом.

### 4.5 Огляд стандартів РГ1

Розглянемо стан стандартів, розроблюваних РГ1.

**ISO/IEC IS 27000:2018** – Information security management systems – Overview and vocabulary (published). Системи менеджменту інформаційної безпеки – Огляд і словник (опублікований).

Для того, щоб полегшити гармонізацію стандартів, що відносяться до РГ1, і забезпечити єдине і чітке їх розуміння, необхідно документувати в одному стандарті основні положення, систематичний словник і набір основних понять і термінів, що використовуються у всій серії стандартів, що відносяться до РГ1.

Даний стандарт є ключовим документом для досягнення ефективності розробки стандартів у РГ1.

**ISO/IEC IS 27001:2013** – Information security management systems – Requirements Системи менеджменту інформаційної безпеки – Вимоги

Цей стандарт утворює серцевину сімейства ISMS стандартів.

Він визначає вимоги для встановлення, реалізації, експлуатації, моніторингу, перегляду, підтримки документованої ISMS в контексті загальних ділових ризиків організації. Він також визначає вимоги до реалізації заходів безпеки, адаптованих до потреб конкретних організацій або їх частин.

**ISO/IEC IS 27006:2015** – Requirements for bodies providing audit and certification of information security management systems (published). Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки.

Цей стандарт визначає вимоги та надає настанови для органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки, на додаток до вимог, що містяться в стандартах ISO/IEC 17021 та ISO / IEC 27001.

**ISO/IEC IS 27002:2013 – Code of practice for information security controls (published).** Практичні правила для заходів з інформаційної безпеки.

ISO/IEC 27002 опублікований, як стандарт, що надає всеохопні настанови щодо реалізації заходів інформаційної безпеки, і безпосередньо підтримує стандарт

ISO/IEC 27001.

**ISO/IEC 27003:2012 – Information security management systems implementation guidance (published).** Настанова з реалізації систем менеджменту інформаційної безпеки.

Цей стандарт безпосередньо підтримує стандарт ISO/IEC 27001 і надає матеріал з настанов, який стосується реалізації ISMS.

**ISO/IEC 27004:2011 – Information security management measurements (published).** Вимірювання менеджменту інформаційної безпеки.

ISO/IEC 27004 запропонований, як стандарт з настанов, який надає можливість вимірювати рівень ефективності реалізованих відповідно до стандарту ISO/IEC 27001 заходів і процесів.

Задля результативності, ISO/IEC 27004 розглядає ряд одиниць вимірювання, що включають результативність заходів. ISO/IEC 27004 також надає такі засоби, які дозволили б ефективно вимірювати діяльність з інформаційної безпеки, яка використовується для захисту інформаційних активів організації.

**ISO/IEC IS 27005:2011 – Information security risk management (published).** Керування ризиками інформаційної безпеки.

Даний стандарт надає посібник з менеджменту ризиків інформаційної безпеки і розглядає принципи менеджменту ризиків інформаційної безпеки, методи оцінки ризиків, трактування ризиків, моніторинг і перегляд ризиків, надаючи додаткову інформацію відносно виконання стандарту ISO/IEC 27001.

**ISO/IEC 27007:2014 – Guidelines for information security management systems auditing (published).** Настанова з аудиту систем менеджменту інформаційної безпеки.

ISO/IEC 27007 запропонований з метою надання настанов з проведення аудитів ISMS, а також настанов з компетентності аудиторів систем менеджменту інформаційної безпеки в доповнення до настанов, які містяться в ISO 19011.

Даний стандарт розглядає окрему настанову, що необхідна для аудитів ISMS в підтримку стандарту ISO/IEC 27006 і загальної настанови для аудиторів, що міститься в ISO 19011.

**ISO/IEC TR 27008:2011 – Guidance for auditors on ISMS controls (published).** Настанова для аудиторів заходів ISMS.

Даний технічний звіт 2-го типу націлений на надання настанови з того, як перевірити доказ і якість заходів, що були реалізовані в ISMS, і тим самим підтримати планування і виконання оцінки заходів ISMS.

**ISO/IEC 27013:2017 – Guidance on the integrated implementation of 20000-1 and 27001 (published).** Настанова з інтегрованої реалізації стандартів ISO/IEC 20000-1 і ISO/IEC 27001.

Даний стандарт надає настанову з реалізації інтегрованої системи менеджменту інформаційної безпеки і менеджменту послугами IT.

**ISO/IEC 27014:2013 – Information security governance framework (published).** Основні положення управління інформаційною безпекою.

Даний стандарт надає основні положення (framework) управління інформаційною безпекою в підтримку вимог до управління корпорацією, які потребують від організації продемонструвати ефективні внутрішні заходи з управління.

**ISO/IEC 27010:2015 – Information security management guidelines for inter-sector communications (published).** Настанови з менеджменту інформаційної безпеки для міжгалузевих зв'язків. Цей стандарт надає настанови менеджменту інформаційної безпеки зв'язків і співробітництву між відкритими і/або закритими секторами.

**ITU X.1051|ISO/IEC 27011: 2018 – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.** Настанова з менеджменту інформаційної безпеки для телекомунікаційних організацій на основі ISO/IEC 27002.

Даний стандарт:

- встановлює настановчі вказівки і загальні принципи для ініціювання, реалізації, підтримки і покращення менеджменту інформаційної безпеки в телекомунікаційних організаціях на основі ISO/IEC 27002;
- надає основу для реалізації менеджменту інформаційної безпеки в телекомунікаційних організаціях для забезпечення конфіденційності, цілісності і доступності телекомунікаційних засобів і послуг.

**ISO/IEC 27015:2012 – Information security management guidelines for financial and insurance services (published).** Настановчі вказівки з менеджменту інформаційної безпеки для фінансових послуг і послуг страхування.

Цей стандарт встановлює вимоги і настановчі вказівки для ініціювання, реалізації, підтримки і покращення менеджменту інформаційної безпеки, специфічні для організацій, які надають фінансові послуги і послуги страхування. Вимоги даного стандарту доповнюють вимоги стандарту ISO/IEC 27001, які також повинні виконуватись.

Настанови є такими, що доповнюють в контексті надання фінансових послуг і послуг страхування загальні настанови з реалізації менеджменту інформаційної безпеки, які надаються стандартом ISO/IEC 27002.

**ISO/IEC 27031:2011 – Guidelines for ICT readiness for business continuity (published).** Настановчі вказівки щодо готовності ІКТ для підтримки неперервності бізнесу.

Даний стандарт описує концепцію і принципи готовності ІКТ для підтримки безперервного бізнесу для будь-якої організації незалежно від її розміру, а також специфікації усіх аспектів покращення готовності ІКТ для забезпечення неперервності бізнесу. Область дії цього стандарту охоплює всі події і інциденти, котрі можуть мати вплив на системи і інфраструктуру ІКТ. Вона включає і розширює практичні правила поведінки з інцидентами безпеки і менеджмент планування підтримки готовності ІКТ.

**ISO/IEC 27033 – Network security (all parts).** Безпека мереж (всі частини).

Різні частини цього стандарту надають детальні настанови з аспектів безпеки, що відносяться до управління і використання мереж інформаційних систем і їх зв’язків.

**ISO/IEC 27034 – Application security (all parts).** Безпека додатків (всі частини).

Різні частини даного стандарту надають настановчі вказівки для розробників програмного забезпечення, адміністраторів безпеки, користувачів програмного забезпечення, аудиторів, менеджерів з визначення, розробки у випадку необхідності, реалізації, підтримки і заміни додатків з точки зору інформаційної безпеки.

**ISO/IEC 27035:2018 – Information security incident management.** Менеджмент інцидентів інформаційної безпеки.

Цей стандарт надає настанову з оцінки ризиків, що виникають від придбання і використання послуг аутсорсингу в підтримку стандарту ISO/IEC 27001 і заходів, пов’язаних з аутсорсингом, стандарту ISO/IEC 27002.

**ISO/IEC 27037:2017 – Guidelines for identification, collection and/or acquisition and preservation of digital evidence).** Настановчі вказівки для ідентифікації, збору і/або придбання і зберігання цифрових доказів.

Даний стандарт надає детальну настанову, яка описує процес для виявлення, ідентифікації, збору і/або придбання і зберігання цифрових даних, котрі можуть містити інформацію, яка має потенційне доказове значення.

**ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:**

1. Що таке стандартизація?
2. Що є найважливішими результатами стандартизації?
3. Назвіть основні вимоги до стандартів, що розробляються.
4. Які типи стандартів ви знаєте?
5. З яких елементів складається стандарт?
6. Назвіть стандарти серії 27000.