УДК 004.056

М. А. Бартко
Н. П. Кухарська
м. Львів, Львівський державний університет безпеки життєдіяльності

АНАЛІЗ МІЖНАРОДНОЇ НОРМАТИВНОЇ ДОКУМЕНТАЦІЇ З ПИТАНЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: СТАНДАРТ ISO/IEC 27001:2013

Управління інформаційною безпекою (ІБ) доволі широко обговорювана тема на міжнародному рівні. Наявність серії міжнародних стандартів, розроблених спільними зусиллями Міжнародної організації з стандартизації (ISO – International Organization for Standardization) і Міжнародної електротехнічної комісії (IEC – International Electrotechnical Commission), підтверджує цей факт.

Розглянемо стандарт ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements [1], який де-факто призначений для побудови системи менеджменту інформаційної безпеки (СМІБ). Остання його версія вийшла восени 2013 року.

В Україні стандарт ISO/IEC 27001 як національний введений в дію з 1 липня 2012 року.

Згідно з положеннями цього стандарту СМІБ повинна мати процесний характер, що відповідає циклу Демінга-Шухарта, який передбачає таку послідовність дій: планування процесу, його реалізація, перевірка, подальші вдосконалення, що полягають у ретельному перегляді підходів з актуалізацією уваги на плануванні, згодом цикл повторюється.

Якщо уважно подивитися на зміст ISO/IEC 27001:2013, то можна виокремити розташовані послідовно один за одним розділи стандарту:

- Planning (Планування);
- Operation (Функціонування);
- Performance evaluation (Оцінка результативності);
- Improvement (Поліпшення),

які і відображають модель Демінга-Шухарта, або, як ще її називають, модель PDCA (Plan-Do-Check-Act). Ця модель може бути застосована при структуруванні всіх процесів СМІБ в будь-якій організації. Система управління інформаційною безпекою, використовуючи як вхідні дані вимоги інформаційної безпеки і очікування зацікавлених сторін, за допомогою необхідних дій і процесів видає вихідні дані – результати по забезпеченню ІБ.

Відповідно до вимог стандарту, керівництво організації повинно визначити межі дії системи менеджменту інформаційної безпеки, після чого сформувати політику управління ІБ, яка визначатиме концептуальні характеристики бізнесу організації, сукупність її активів і застосовуваних інформаційних технологій. Організація також повинна чітко визначити зацікавлені сторони (interested parties) і їх вимоги. На межі СМІБ безпосередньо впливають вимоги законодавства, регулюючих органів, контрактні зобов'язання, тощо. Межі СМІБ мають бути оформлені у вигляді окремого документа, включаючи опис контексту організації. Наступним ключовим етапом повинна бути оцінка ризиків і вибір методу їх обробки, з метою формування єдиної в організації системи поглядів на питання забезпечення і управління ІБ. Наступний етап полягає у виявленні ризиків відповідно до обраного, придатного для конкретної організації методу. Виявлення ризиків здійснюється на основі формування переліку активів і їх власників, з метою виявлення слабких місць активів, вразливості яких можуть спричинити реалізацію загроз інформаційної безпеки.

Наступним проміжним етапом є оцінка виявлених ризиків і формування стратегії управлінням ними, яка може полягати в:

- зміні параметрів захисту та\або управління;
- прийнятті ризиків, у разі задоволення умов інформаційної політики;
- позбавленні від ризиків;
- покладанні відповідальності за ці ризики на сторонні організації, або передачі ризиків.

У результаті прийняття певної стратегії управління ризиками має відбуватися, відповідно до стандарту, зниження рівня ризику до прийнятного рівня – залишкового ризику. Таким чином СМІБ організації є задокументованою і готовою для впровадження.

Згідно з положеннями ISO/IEC 27001 процес реалізації та експлуатації системи менеджменту інформаційної безпеки повинен полягати в:

1. Формулюванні плану обробки ризиків.
2. Реалізації плану обробки ризиків.
3. Формуванні і застосуванні засобів управління.
4. Оцінці ефективності прийнятих засобів управління.
5. Підготовці і здійсненні плану підвищення обізнаності персоналу.
6. Управлінні діяльністю системи менеджменту інформаційної безпеки.
7. Управлінні ресурсами системи менеджменту інформаційної безпеки.
8. Впровадженні в дію систем виявлення інцидентів інформаційної безпеки.

Вищеописані дії, відповідно до циклу Демінга-Шухарта, є процесами планування і здійснення. Після них повинні йти процеси перевірки і перегляду попередніх дій (вдосконалення), які і описує решта частина стандарту.

У стандарті особлива увага приділяється процесам документування вимог і політик організації у сфері ІБ і їх захисту, а також формалізації механізмів реагування на інциденти інформаційної безпеки. Управління записами передбачає постійне ведення журналів, протоколів і форм дозволу доступу, пов'язаних як з активами і їх ризиками, так і з процесами забезпечення ІБ організації.

Вдосконалення СМІБ згідно стандарту повинно здійснюватися на основі результатів проведення окремої процедури – внутрішнього аудиту системи, метою якої є перевірка відповідності системи бізнес-вимогам, ефективності механізмів управління інформаційною безпекою та коректності виконання функцій захисту. Результатом проведення аудиту має бути аналітичний висновок про можливість поліпшення, доповнення або видозміни системи, що сприятиме подальшому розвитку СМІБ.

ISO/IEC 27001:2013 вимагає чіткого планування завдань, в ході якого фіксується:

- що має бути зроблено;
- які ресурси будуть потрібні;
- хто відповідає;
- терміни;
- як будуть оцінюватися результати виконання завдань.

Основна мета додатку А, що міститься в стандарті, – формалізовано представити цілі і засоби управління інформаційною безпекою. У новій версії стандарту подано перелік 114 контролів (контроль – це спосіб мінімізації ризику інформаційної безпеки), що розділені на 14 доменів: політики інформаційної безпеки; організаційні питання ІБ; питання ІБ, пов'язані з персоналом; управління активами; управління доступом; криптографія; фізична безпека і захист від загроз навколишнього середовища; операційні питання ІБ; безпека комунікацій; приймання, розробка та підтримка інформаційних систем; взаємодія з постачальниками; управління інцидентами ІБ; питання ІБ при забезпеченні безперервності бізнесу; виконання вимог.

По суті стандарт ISO/IEC 27001:2013 описує механізми вибору контролів на основі оцінки ризиків, містить перелік контролів, що слугує таким собі мінімумом, на базі якого і будується система менеджменту інформаційної безпеки.

Список літератури:

1. Standard ISO/EC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.