АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ В СФЕРІ КАДРОВОЇ БЕЗПЕКИ

Аванесова Н.Е., д.е.н., проф.,
Марченко О.В., к.е.н., доц.,
Харківський національний університет будівництва та архітектури

Як і інші економічні системи, система забезпечення кадрової безпеки функціонує в межах законодавчого та правового поля, що є неодмінною умовою її ефективності [7].

Досліджуючи нормативно-правові умови забезпечення кадрової безпеки діяльності суб'єктів господарювання, слід звернути увагу, що якогось спеціального законодавства на сьогоднішній день в Україні не існує. Проте є законодавчі акти та нормативно-правові документи, що здійснюють опосередкований вплив на кадрову безпеку суб'єктів господарювання, а також внутрішні положення та регламенти.

Також можна виділити основні міжнародні стандарти, які впливають на забезпечення кадрової безпеки [1,8]: ISO 15408 «Загальні критерії оцінки безпеки інформаційних технологій»; ISO 27001 «Система управління інформаційною безпекою»; ISO 31000:2018 «Управління ризиками. Принципи та рекомендації».

Оскільки захист інформації є одним із найактуальніших завдань в контексті забезпечення кадрової безпеки, тому міжнародний багаточастинний стандарт ISO 15408 є одним із найбільш поширених стандартів у сфері безпеки.

Перша частина стандарту ISO/IEC 15408-1:2009 (ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель) [2] встановлює принципи та критерії оцінювання безпеки інформаційних технологій, а також визначає загальну модель оцінки їх безпеки, надану різними частинами даного стандарту.

Друга частина стандарту ISO/IEC 15408-2:2008 (ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги) [2] визначає зміст та вимоги до функціональних компонентів безпеки в комп'ютерній системі, що мають бути оцінені. Також він дає рекомендації відносно специфікації індивідуальних вимог безпеки, якщо немає відповідних завчасно визначених функціональних компонентів безпеки. В стандарті міститься повний каталог завчасно визначених функціональних

компонентів безпеки, які систематизовано з використанням ієрархічної структури класів, сімей та компонентів.

Третя частина стандарту ISO/IEC 15408-3:2008 (ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки) [3] визначає загальні вимоги, які стосуються критеріїв довіри до безпеки в комп'ютерній системі. Даний стандарт визначає вимоги довіри до безпеки (а також дає рекомендації щодо формування нових вимог), які представлено в ієрархічному порядку в формі класів, сімей і компонентів.

Інформаційна безпека в організації є тією системою, яка потребує комплексного управління, включаючи весь персонал (особливо вищої ланки), інформаційні системи й різноманітні бізнес-процеси. Захист інформації, своєчасне виявлення ризиків безпеки й загроз інформаційним активам організації значною мірою залежить від встановлення певних стандартів. ISO/IEC 27001 (ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги) [5] є основним стандартом системи управління інформаційною безпекою [9]. Першочерговими цілями даного стандарту є: своєчасне виявлення потенційних вразливих місць інформаційної безпеки та загроз інформаційним активам; визначення адекватних засобів мінімізації ризиків та збереження їх в межах допустимого рівню; систематичний та безперервний контроль забезпечення інформаційної безпеки тощо.

Оскільки ризик-менеджмент має фундаментальне значення для управління організацією, відповідно постійно вдосконалюються і підходи до управління ризиками. З цією ціллю Міжнародною організацією зі стандартизації (ISO) було переглянуто стандарт ISO 31000:2009 «Менеджмент ризику» та представлено його оновлену версію ISO 31000:2018 (ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови) [6]. Оновлений документ дає загальне уявлення щодо того, як розробляється, впроваджується та підтримується ефективна система управління ризиками в межах певної галузі, підприємства та ін. Стандарт надає ще більш чіткі вказівки стосовно використання принципів управління ризиками задля вдосконалення процесу планування та прийняття більш ефективних та зважених управлінських рішень.

Таким чином, можна зробити висновок, що в Україні приділяється значна увага впровадженню міжнародних стандартів, які

впливають на забезпечення кадрової безпеки, тому певне підґрунтя захисту прав та інтересів підприємців поступово формується. Однак відсутньою є комплексна законодавча база, яка здатна ефективно забезпечувати безпеку підприємницької діяльності.

Література.

1. Гладун А.Я., Хала К.О. Таксономія стандартів інформаційної безпеки. *Наука, технології, інновації.* 2017. №2. С.53-64. URL: http://nti.ukrintei.ua/wp-content/uploads/2018/05/2017-2_stat7_UA_povn.pdf

2. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель. Чинний від 01.10.2017. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=72376

3. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги. Чинний від 01.10.2017. URL: http:// online.budstandart.com/ua/catalog/doc-page.html?id_doc=72377

4. ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки. Чинний від 01.10.2017. URL: http:// online.budstandart.com/ua/catalog/doc-page.html?id_doc=72378

5. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги. Чинний від 01.01.2017. URL: http:// online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910

6. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови. Чинний від 01.01.2019. URL: http:// online.budstandart.com/ua/catalog/doc-page.html?id_doc=80322

7. Марченко О.В. Підходи до визначення сутності кадрової безпеки та її ключових ознак. *Бізнес-Інформ.* 2019. №7. С.337-344.

8. Панченко В.А. Місце кадрової безпеки в системі економічної безпеки підприємств. *Науковий вісник Ужгородського національного університету.* 2018. №21. Ч.2. С.53-60. URL: http:// nti.ukrintei.ua/wp-content/uploads/2018/05/2017-2_stat7_UA_povn.pdf

9. Система управління інформаційною безпекою ISO 27001 URL: