УДК 006.042

Хоменко І.І., студентка гр. УБіт-14-1,
Науковий керівник: Галушко С.О., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет» м. Дніпро, Україна)

РОЗВИТОК СТАНДАРТІВ БЕЗПЕКИ

Існує єдиний спосіб оцінити захищеність систем – розробити стандарт, що регламентує концепції інформаційної безпеки, вимоги до систем і шляхи їх реалізації, надає систему критеріїв і процедуру оцінювання систем за цими критеріями.

Розроблені та затверджені стандарти інформаційної безпеки створюють базу для погодження вимог розробників систем, споживачів і експертів, що оцінюють захищеність інформації.

Стандарти інформаційної безпеки існують трохи більше двадцяти років. У світі розробка стандартів, технічних звітів, керівництв та рекомендацій в галузі ІБ проводиться безперервно; послідовно публікуються проекти і версії стандартів, присвячених тим чи іншим аспектам інформаційної безпеки на різних стадіях узгодження і затвердження. Деякі стандарти поетапно заглиблюються і деталізують у вигляді сукупності взаємозв'язаних концепціями і структурами груп стандартів. Розробка нормативних документів з інформаційної безпеки, повністю або частково присвячених керуванню інцидентами інформаційної безпеки, здійснюється низькою спеціалізованих міжнародних організацій і консорціумів, таких як, наприклад: CERT, ISO, IEC, IETF, ITU-T, IEEE, OMG, SANS Institute тощо. Значна робота щодо стандартизації питань інформаційної безпеки, зокрема керування інцидентами, проводиться спеціалізованими організаціями і на національному рівні, в першу чергу в США – NIST, CMU/SEI; Німеччині та Великобританії – BSI. Все це дозволило сформувати обширну нормативно - методологічну базу у вигляді міжнародних, національних та галузевих стандартів, а також нормативних і керівних матеріалів, що регламентують діяльність в сфері керування інцидентами інформаційної безпеки. Проте, як свідчить сучасна практика, найважливішу роль в світі відіграють стандарти ISO. Основні з них: ISO 9000, ISO 9001, ISO 9004 (менеджмент якості); ISO 10001, ISO 10002, ISO 10003, ISO 10004 (задоволеність споживачів); EN 9100 (СМК в аерокосмічній галузі); ISO/TS 16949 (СМК в автомобілебудуванні); ISO 14001 (екологічний менеджмент); OHSAS 18001 (професійна безпека); ISO 31000 (менеджмент ризиків); ISO 20000 (СМК IT- послуг); ISO 22000 (продовольча безпека); ISO 26000 (соціальна відповідальність); ISO 50000 (системи менеджменту в енергетиці); ISO 27001 (інформаційна безпека). Усі вони, як основу керування підконтрольними процесами, використовують процесний підхід, що розглядає керування як процес, а саме як набір взаємозалежних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього.

У порівнянні з динамікою розвитку міжнародних стандартів, технічних звітів та рекомендацій з керування інцидентами інформаційної безпеки, в України використання та створення відповідної нормативно-методологічної бази знаходиться на початковій стадії та потребує подальшого розвитку. Несистематична та неістотна підготовка до реагування та обробки інцидентів інформаційної безпеки призводить до того, що на практиці реагування виявляється хаотичним, невпорядкованим та неефективним, істотно ускладнюючи відновлення бізнес-процесів (технічної експлуатації, менеджменту якості, надання послуг тощо) і через це – потенційно підсилює завданий збиток. Без своєчасної реакції на інциденти інформаційної безпеки та усунення їхніх наслідків неможливо ефективне функціонування системи керування інформаційною безпекою. Суть

методологічно-правильного процесу керування інцидентами ІБ – це чітке визначення ролей та розподіл відповідповідальності щодо якісного та своєчасного реагування на інциденти інформаційної безпеки. Стандартизований методологічний підхід до впровадження процесів керування інцидентами інформаційної безпеки дає можливість організаційно-технічній системі одержати наступні переваги:

•зниження негативного впливу інцидентів інформаційної безпеки на інформаційні процеси;

•прозорість контролю за ефективністю функціонування системи керування інформаційною безпекою;

•доступність моніторингу та оперативної управлінської інформації щодо функціонування системи керування інформаційною безпекою;

•превентивне визначення заходів щодо поліпшення системи керування інформаційною безпекою;

•ефективність взаємодії взаємопов’язаних підсистем керування якістю, послугами, ІБ та інцидентами.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO 9000, ISO 9001, ISO 9004 (менеджмент якості); ISO 10001, ISO 10002, ISO 10003, ISO 10004 (задоволеність споживачів); EN 9100 (СМК в аерокосмічній галузі); ISO/TS 16949 (СМК в автомобілебудуванні); ISO 14001 (екологічний менеджмент); OHSAS 18001 (професійна безпека); ISO 31000 (менеджмент ризиків); ISO 20000 (СМК ІТ-послуг); ISO 22000 (продовольча безпека); ISO 26000 (соціальна відповідальність); ISO 50000 (системи менеджменту в енергетиці); ISO 27001 (інформаційна безпека).