ВСТУП

Метою інформаційної безпеки є забезпечення неперервної роботи організації та мінімізація розміру збитків (втрат) від подій, що є загрозою безпеці, шляхом їх нейтралізації. Система менеджменту інформаційної безпеки дає змогу використовувати інформацію, забезпечуючи при цьому її захист, а також захист інформаційних та комунікаційних ресурсів.

Інформаційна безпека складається із трьох основних компонентів:

а) конфіденційність – захист конфіденційної інформації від несанкціонованого доступу;

б) цілісність – забезпечення точності та повноти інформації та комп'ютерних програм;

в) доступність – забезпечення доступності інформації та необхідних послуг для користувачів.

Інформація існує у різних формах. Її можна зберігати на комп'ютерах, передавати обчислювальними мережами, роздруковувати або записувати на папері, а також озвучувати у розмовах. З погляду безпеки всі види інформації, зокрема паперова документація, бази даних на цифрових носіях, розмови та інші засоби передавання знань чи ідей потребують надійного захисту.

Інформація та інформаційні системи, мережі, в яких вона функціонує, є важливими ресурсами організації. Їх доступність, цілісність та конфіденційність можуть мати особливе значення для забезпечення конкурентоздатності організації, руху коштів, рентабельності, відповідності правовим нормам та іміджу організації. Сучасні організації сьогодні не убезпечені від порушення режиму безпеки, що зумовлено низкою факторів. Інформаційним системам та мережам властиві такі загрози, як фізичне пошкодження/втрата (будівлі, обладнання, інформації); компрометація інформації; викривлення/підроблення інформації і/або даних, внаслідок пожежі, крадіжки, неконтрольованого ремонту, збоїв електроживлення, недбалості персоналу, відмови телекомунікаційного обладнання, несанкціонованого використання обладнання/програмного забезпечення, віддаленого шпіонажу, перехоплення побічних електромагнітних випромінювань та наведень, розкриття/продажу інформації працівниками організації, зловживання працівником правами доступу до інформації, підроблення прав доступу до інформації, отримання несанкціонованого доступу до інформації зовнішніми зловмисниками, неправильної роботи системи захисту інформації, навмисного невикористання системи захисту інформації, компрометації паролів доступу, помилок у програмному забезпеченні тощо.

З кожним днем з'являються нові загрози, які здатні нанести збитків організації. Це зокрема хакерські дії, соціальна інженерія, втручання до системи, злом, несанкціонований доступ до системи, комп'ютерні злочини, продаж інформації, спуфінг,

руйнування інформаційної системи, атаки на систему (наприклад, розподілена відмова в обслуговуванні), перегляд інформації з обмеженим доступом, фальсифікація та підроблення даних, зловмисні коди (віруси, логічні бомби, “троянські коні” тощо), продаж персональної інформації, дефекти системи тощо. Можна стверджувати, що такі загрози з часом набуватимуть все більшого поширення.

Водночас, внаслідок посилення залежності організацій від інформаційних, комунікаційних систем та послуг вони можуть стати вразливішими до порушень режиму безпеки. Поширення інформаційних та комунікаційних систем надає все нові можливості для несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості спеціалістів централізовано контролювати інформаційні системи та мережі.

Захисні заходи є ефективнішими, якщо вони вбудовані в інформаційні системи та послуги на етапах формування технічного завдання та проектування. І що швидше організація запровадить заходи із захисту своїх інформаційних і комунікаційних систем, то ефективнішими та дешевими вони будуть у майбутньому.

У запропонованому Вашій увазі навчальному посібнику детально аналізується процедура менеджменту інформаційної безпеки на основі міжнародних стандартів. Міжнародна організація зі стандартизації (ISO – International Organization for Standardization) [1] та Міжнародна електротехнічна комісія (IEC – International Electrotechnical Commission) [2] утворюють спеціалізовану систему всесвітньої стандартизації. Державні органи, які є членами ISO або IEC, беруть участь у розробленні міжнародних стандартів за допомогою технічних комітетів, які засновані відповідною організацією для того, щоб сприяти розвитку стандартизації та суміжних видів діяльності у світі для міжнародного обміну товарами і послугами, а також розвитку співробітництва в інтелектуальній, науково-технічній та економічній сферах діяльності. Технічні комітети ISO та IEC співпрацюють у галузях взаємного зацікавлення. Інші міжнародні організації, урядові та неурядові, що контактують з ISO та IEC, також беруть участь у цій роботі.

Проекти міжнародних стандартів складають відповідно до правил, які визначені директивами ISO/IEC (частина 2).

У галузі інформаційних технологій ISO та IEC заснували Спільний технічний комітет (JTC – Joint Technical Committee 1), ISO/IEC JTC 1. Проекти міжнародних стандартів, які приймає об’єднаний технічний комітет, розсилаються державним органам для голосування. Щоб опублікувати документ як міжнародний стандарт, необхідно хоча б 75 % голосів членів-організацій, які беруть участь у голосуванні [3, 4].

Сьогодні існує велика кількість сфер менеджменту: виробництво, фінанси, продаж/закупівля, персонал тощо. Завдяки розвитку сучасного високотехнологічного функціонування організацій поступово усвідомлюється важливість і таких сфер, як інформаційні технології, інформаційна безпека, системи менеджменту інформаційної

безпеки, якість та навколишнє середовище. Про це свідчить зростаюча популярність у всьому світі відповідних міжнародних стандартів серії ISO 27000 [5], ISO 20000 [6], ISO 9000 [7] та ISO 14001 [8]. Основні принципи менеджменту загалом для всіх сфер менеджменту є схожими. Тому відповідні системи менеджменту доповнюють одна одну, утворюючи інтегровані системи менеджменту організації (IMS – Integrated Management Solutions) [9].

Існує три основні групи вимог до системи безпеки в довільній організації.

Перша група вимог – це унікальний набір ризиків порушення безпеки, що складається із загроз інформаційним ресурсам та їх вразливостей та можливого впливу цих ризиків на функціонування організації. Більшу частину таких ризиків описано у цьому посібнику. Ризикам можна сміливо протистояти, якщо діяти за вимогами стандартів менеджменту інформаційної безпеки. Проте існують ризики, що вимагають спеціального підходу, і їх необхідно розглядати з врахуванням оцінки кожної конкретної організації чи кожного конкретного компонента інформаційної системи.

Друга група вимог – це набір правових та договірних вимог, яких має дотримуватися організація, її партнери, підрядники та постачальники послуг; у цьому разі зростає необхідність стандартизації із поширенням електронного обміну інформацією у мережах між організаціями. Правила міжнародних стандартів можуть слугувати надійною основою для визначення загальних вимог цього типу.

Третя група вимог – це унікальний набір принципів, цілей та вимог до оброблення інформації, який розробила організація для виробничої мети. Важливо (наприклад, для забезпечення конкурентоздатності), щоб у політиці безпеки було відображено ці вимоги, а також, щоби наявність чи відсутність засобів менеджменту безпеки в інформаційній інфраструктурі не суперечили меті виробничої діяльності організації.

У практичних правилах менеджменту інформаційної безпеки наведено за можливості вичерпні рекомендації. Їх мета – слугувати довідником для визначення засобів контролю інформаційної безпеки, що існують у фінансовій сфері, промисловості та торгівлі, а, відповідно, можуть застосовуватися великими, середніми та малими організаціями. Враховуючи зростаючу роль електронного передавання даних по мережах між організаціями, очевидною є користь від єдиного довідкового документа з систем менеджменту інформаційною безпекою. Він дає змогу встановити взаємну довіру між організаціями, що об’єднані у корпоративну мережу, їх торговими партнерами, а також становитиме основу для менеджменту інформаційних ресурсів.

Не всі описані засоби контролю підходять для довільної організації. Окрім того, вони не в стані врахувати всі обмеження локального характеру, що накладаються навколишнім середовищем та технологіями. Не можуть вони також задовольняти за формою всіх користувачів організації. Відповідно, запропоновані правила необхідно застосовувати творчо. Такі правила слугують лише основою для розроблення на їх основі унікальної системи менеджменту інформаційної безпеки організації.

Цей посібник призначений для студентів, які навчаються за напрямом “Інформаційна безпека”, а також керівників організацій та підприємств, начальників служб захисту інформації організацій, інженерів та інших спеціалістів у галузі інформаційної безпеки.

Метою посібника є формування необхідних знань у вищезгаданих осіб для ефективної побудови системи менеджменту інформаційної безпеки.

Оскільки неможливо запропонувати вирішення завдань побудови системи менеджменту інформаційної безпеки, які були б однаковими для всіх типів підприємств, організацій тощо, у посібнику розглянуто основні принципи побудови такої системи без надмірної деталізації. На основі наведених принципів та рекомендацій залежно від мети розробників системи менеджменту інформаційної безпеки для конкретного підприємства чи організації, а також із врахуванням власного бачення, розробники зможуть ефективно вирішити поставлене завдання.