УДК 65.012.8

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Горяна Ольга Гарріївна
ДВУЗ «Національний гірничий університет», http://bit.nmu.org.ua, goryanaolga@gmail.com

У даній статті розглядається система управління інформаційною безпекою за стандартом ISO 27001. Стандарт містить вимоги в галузі інформаційної безпеки для створення, розвитку і підтримки системи менеджменту інформаційної безпеки.

Ключові слова – Стандарт, ISO 27001, управління, інформаційна безпека.

ВСТУП

Інформація є одним із головних ділових ресурсів, який забезпечує організації додану вартість, і внаслідок цього потребує захисту. Слабкі місця в захисті інформації можуть призвести до фінансових втрат, і нанести збиток комерційним операціям. Тому в наш час питання розробки системи управління інформаційною безпекою та її впровадження в організації є концептуальною.

Стандарт ISO 27001 визначає інформаційну безпеку як: «збереження конфіденційності, цілісності та доступності інформації».

ISO 27001:2005 являє собою перелік вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації, а стандарт ISO 27002:2005 виступає в якості керівництва по впровадженню, яке може використовуватися при проектуванні механізмів контролю, вибраних організацією для зменшення ризиків інформаційної безпеки.

Стандарт ISO 27001 визначає процеси, що представляють можливість бізнесу встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки; встановлює вимоги до розробки, впровадження, функціонуванню, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації [3].

МОЖЛИВОСТІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Система управління інформаційною безпекою на основі стандарту ISO 27001 дозволяє:

- зробити більшість інформаційних активів найбільш зрозумілими для менеджменту компанії;
- виявляти основні загрози безпеки для існуючих бізнес-процесів;
- розраховувати ризики і приймати рішення на основі бізнес цілей компанії;
- забезпечити ефективне управління системою в критичних ситуаціях;
- проводити процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі інформаційної безпеки);
- чітко визначити особисту відповідальність;
- досягти зниження і оптимізації вартості підтримки системи безпеки;
- полегшити інтеграцію підсистеми безпеки в бізнес-процеси і інтеграцію з ISO 9001:2000;
- продемонструвати клієнтам, партнерам, власникам бізнесу свою прихильність до інформаційної безпеки;
- отримати міжнародне визнання і підвищення авторитету компанії, як на внутрішньому ринку, так і на зовнішніх ринках;
- підкреслити прозорість і чистоту бізнесу перед законом завдяки відповідності стандарту [1].

Поряд з елементами управління для комп’ютерів і комп'ютерних мереж, стандарт приділяє велику увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам.

Вимоги цього стандарту мають загальний характер і можуть бути використані широким колом організацій - малих, середніх і великих - комерційних і промислових секторів ринку: фінансовому та страховому, у сфері телекомунікацій, комунальних послуг, у секторах роздрібної торгівлі і виробництва, різних галузях сервісу, транспортній сфері, органах влади та багатьох інших.

Стандарт ISO 27001 гармонізований зі стандартами систем менеджменту якості ISO 9001:2000 та ISO 14001:2004 і базується на основних принципах. Більш того, обов'язкові процедури стандарту ISO 9001 потрібні і стандартом ISO 27001. Структура документації по вимогам ISO 27001 аналогічна структурі за вимогам ISO 9001. Велика частина документації, потрібна по ISO 27001, вже могла бути розроблена, і могла використовуватися в рамках ISO 9001. Таким чином, якщо організація вже має систему менеджменту відповідно, наприклад, з ISO 9001 та ISO 14001), то краще забезпечувати виконання вимоги стандарту ISO 27001 в рамках вже існуючих систем, що передбачає значне зниження внутрішніх витрат підприємства та вартості робіт щодо впровадження та сертифікації [2].

За стандартом ISO 27001:2005 проводиться міжнародна сертифікація системи управління інформаційною безпекою.

Сертифікація на відповідність стандарту дозволяє наочно показати діловим партнерам, інвесторам і клієнтам, що в компанії захист інформації поставлено на високий рівень і налагоджено ефективне управління інформаційною безпекою.

ЕТАПИ РОЗРОБКИ І ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІБ

Можна виділити наступні основні етапи розробки системи управління ІБ:

- інвентаризація активів;
- категорювання активів;
- оцінка захищеності інформаційної системи;
- оцінка інформаційних ризиків;
- обробка інформаційних ризиків (у тому числі визначення конкретних заходів для захисту цінних активів);
- впровадження вибраних заходів обробки ризиків;
- контроль виконання та ефективність вибраних заходів;
- роль керівництва компанії в системі управління ІБ [1].

Одним з основних умов ефективного функціонування системи управління ІБ є залучення керівництва компанії в процес управління ІБ. Всі співробітники повинні розуміти, що, по-перше, вся діяльність по забезпеченню ІБ ініційована керівництвом і обов'язкова для виконання, по-друге, керівництво компанії особисто контролює функціонування системи управління ІБ, по-третє, саме керівництво виконує ті ж правила по забезпеченню ІБ, що і всі співробітники компанії.

НАВЧАННЯ СПІВРОБІТНИКІВ КОМПАНІЇ

Для ефективного впровадження системи управління інформаційної безпеки на підприємстві, необхідно не тільки виконати всі розробки і впровадження, а також провести навчання співробітників.

Навчання співробітників можна виконувати у формі очних та заочних курсів з подальшим тестуванням, доцільно організувати навчанням співробітників за допомогою системи дистанційного навчання, в рамках якого можуть бути представлені різні курси (як для користувачів, так і для фахівців), ігрові методики навчання.

Основна складність може полягати у перевірці ефективності процедур системи управління ІБ. Тобто для кожної процедури необхідно розробити критерії, за якими буде перевірятися її ефективність, і, крім цього, такі критерії потрібно розробити для всієї системи управління в цілому [2].

ВИСНОВКИ

СУІБ і сертифікація на відповідність стандарту ISO 27001 дає компанії такі переваги, як управління інформаційною безпекою компанії в рамках єдиної корпоративної політики, управління ризиками та їх своєчасне виявлення, зниження ризиків від зовнішніх і внутрішніх загроз, систематизація процесів забезпечення ІБ, встановлення пріоритетів компанії в області ІБ. У свою чергу це забезпечує компанії конкурентну перевагу, демонструючи здатність керувати інформаційними ризиками, при цьому також збільшується капіталізація компанії.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO 27001:2005 «Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційною безпекою - Вимоги».

2. Ярочкин В.І. Безпека інформаційних систем. - М.: вид. "Вісь-89", 2006.

3. Ярочкин В.І. Система безпеки фірми. - М.: вид. "Вісь-89", 2008.