Information Assets Description Methods in Creating Information Security Management System

Taras Kret

Information Security Department,
Lviv Polytechnic National University,
UKRAINE, Lviv, S. Bandery Str., 12,
E-mail: kret.tb@gmail.com

Information security – 80% management and 20% technology. The study of information security management is promising for advanced studies.

Management of information security described in ISO / IEC 27001:2005, ISO/ IEC 13335-3-2007. These standards specify the requirements and methods of management of information security. The organization is certified according to international standards has great advantages

Description of information assets is a major during the certification. At this stage, created information database. This information database is information assets. Information security policy will be applied to this base.

Information assets are the main features of financial and material assets. But they are more valuable. Scale graduation is also of great value when you create information security management system. Base information assets must consist of names, persons responsible and the location of assets.

One of the main conditions for effective functioning of information security management is to involve management of the creation and operation of the system. Employees should understand that the rules of information security management system is obligatory for execution. Managers should set an example.

Methods of describing information assets is the basis of reliable information security management system. Register of assets is a table which shows the existing assets. Create groups of assets allows grouping similar assets and simplify work with them. When creating a methodology describing information assets used by the process approach and model «Plan-Do-Check-Act». Implement continuous process improvement information security organization.

Методика опису інформаційних активів організації при створенні системи менеджменту інформаційної безпеки

Тарас Крет

Кафедра захисту інформації,
Національний університет "Львівська політехніка",
УКРАЇНА, м.Львів, вул.С.Бандери, 12,
E-mail: kret.tb@gmail.com

Запропоновано методику опису інформаційних активів організації при створенні ефективної системи менеджменту інформаційної безпеки (СМІБ) на основі сімейства міжнародних стандартів ISO/IEC 27001 та ISO/IEC 13335. Головною метою створення методики на основі цих стандартів є вдосконалення СМІБ організації.

Ключові слова – захист інформації, системи менеджменту інформаційної безпеки, опис активів.

I. Вступ

На сьогоднішній день інформаційна безпека – це 80 % менеджменту та 20 % технології.

Міжнародні стандарти ISO/IEC 27001:2005, ISO/IEC 13335-3-2007 встановлюють вимоги та методи до систем менеджменту інформаційної безпеки (СМІБ) та дозволяють структурувати процеси управління інформаційною безпекою. Під час їх реалізації першим та головним завданням є опис інформацій активів організації [1].

При створенні методики опису інформаційних активів використано процесний підхід та модель «Plan-Do-Check-Act» (цикл Шухарта-Деминга), тобто реалізується безперервне поліпшення процесу інформаційної безпеки організації [2].

II. Інформаційні активи

Об'єктом СМІБ є інформаційні активи, тобто матеріальні або нематеріальні об'єкти, які є інформацією або містять інформацію, або необхідні для оброблення інформації. Наприклад, одним активом є: системний блок + монітор + клавіатура + мишка + всі електронні документи, які розміщенні на дисках ПК + все програмне забезпечення, яке встановлене на ПК.

Інформаційні активи – це:

- бази даних і файли даних;
- договори і домовленості;
- системна документація;
- науково-дослідна інформація;
- довідкова інформація, методичні вказівки, інструкції;
- навчальний матеріал;
- процедури експлуатації;
- плани забезпечення неперервності функціонування;
- заходи щодо ліквідації неполадок;
- контрольні журнали;

- архівна інформація.

Інформаційні активи володіють основними властивостями фінансових і матеріальних активів підприємства. Загалом цінність інформаційних активів набагато більша за фінансові активи підприємства.

Захист інформаційних активів залишається одним з пріоритетних на сьогоднішній день.

III. Методика опису інформаційних активів

Запропонована методика на основі стандартів ISO/IEC 27001:2005, ISO/IEC 13335-3-2007 передбачає створення реєстру інформаційних активів організації.

Згідно методики створюється реєстр активів, тобто подається розгорнута таблиця в якій відображаються існуючі активи організації (таблиця).

Під час опису активів використовуються такі атрибути:

- назва активу;
- рівні забезпечення;
- максимальний час недоступності;
- власник активу;
- місце знаходження активу;
- категорія активу.

Найкраще використовувати типові (стандартні) назви активів. Наприклад, «Персональний комп'ютер бухгалтерії №12» можна задекларувати так: «ПК №12 тип Б». Це дає змогу отримати в результаті просту і наочну таблицю.

Виділяють такі три рівні забезпечення: конфіденційності, цілісності, доступності, тобто необхідно оцінити можливі втрати, що понесе організація. Шкалу рівнів забезпечення можна виконувати в грошовому еквіваленті та за допомогою системи рівнів. Для базової оцінки ризиків достатньо трьох рівневої шкали оцінки градації (низький, середній, високий).

При виборі рівнів забезпечення слід враховувати:

- чим менша кількість рівнів, тим нижча точність оцінки;
- чим більша кількість рівнів, тим складнішим стає оцінювання.

Виходячи з данного твердження потрібно сказати, що надмірно велика градація ризиків активів не завжди є доцільною [3].

Максимальний час недоступності – час на протязі якого дозволяється недоступність інформаційного активу.

Власником активу варто призначати особу, яка реально працює з активом і здатна впливати на властивості і стан активу.

Місцезнаходження активу найчастіше визначають територіально відповідно до проекту будівлі. Наприклад, «корпус №5», «Бухгалтерія», «НДЧ».

Категоріювання активів дає змогу згрупувати схожі активи і спростити роботу з ними. Такими категоріями можуть бути: «Паперові документи (ПД)», «Електронні документи (ЕД)», «Програмне забезпечення (ПЗ)», «Комп'ютерна техніка (КТ)», «Мережеве обладнання (МО)», «Допоміжне обладнання (ДО)», «Персонал (П)», «Віртуальна інформація (ВІ)» [4].

Реєстр активів

Назва активу	Необхідність забезпечення			Максимальний час недоступності	Власник активу	Місцезнаходження активу	Категорія активу
	К	Ц	Д				

Даний процес створює певну складність, оскільки цінність активів оприділяється на основі експертних оцінок їх власників. На даному етапі часто проводять обговорення між консультантами по розробці системи безпеки та власником активів. Це дозволяє власникам активів, зрозуміти яким чином слід визначити вартість активів з точки зору інформаційної безпеки. Для власників активів розробляють різні методи оцінки.

На даному етапі можна використати, наприклад, метод Делфі. Особливістю якого є: наочність, многорівнева структура та анонімність. Цей метод ґрунтується на послідовності дій таких, як опитування, інтерв'ю, мозковий штурм. Головне добитися максимального консенсусу при визначенні правильного рішення.

Базовим принципом методу являється те, що певна кількість незалежних експертів краще оцінює і передбачає результат, чим структурована група особистостей [5].

Висновок

Під час застосування стандартів ISO/IEC 27001:2005 та ISO/IEC 13335-3-2007 слід звертати особливу увагу на опис інформаційних активів організації.

В даній роботі запропоновано методику опису інформаційних активів під час створення СМІБ. Дана методика дає змогу, враховуючи підходи міжнародних стандартів, службі Захисту інформації організації підвищити ефективність функціонування (швидкодія, точність, вартість).

Література

[1] Міжнародний стандарт ISO/IEC 27001:2005 «Інформаційні технології. Методи захисту. Системи менеджменту захисту інформації. Вимоги».

[2] Міжнародний стандарт ISO/IEC 13335-3-2007 «Інформаційні технології. Методи і засоби забезпечення безпеки. Частина 3. Методи менеджменту безпеки інформаційних технологій».

[3] [Електронний ресурс]. – режим доступу: http://bugtraq.ru/library/security/practicaliso.html

[4] [Електронний ресурс]. – режим доступу: http://www.tuv-sud.com.ua/ukraine/ua

[5] http://ru.wikipedia.org/wiki/Метод_Дельфи