УДК 33:659

Д.О. Сікорський

аспірант
Київський національний університет імені Тараса Шевченка

ПОБУДОВА ПРОЦЕСУ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МІЖНАРОДНОГО СТАНДАРТУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В статті наведено аналіз Міжнародного стандарту з інформаційної безпеки ISO / IEC 27001, зокрема нової редакції 2013 р. Здійснено порівняння структури двох варіантів стандарту та викладено можливості нового стандарту. Проведений аналіз є основою для побудови моделей оцінювання інформаційного ризику. Гармонізація ISO / IEC 27001:2013 з усіма сучасними стандартами, випущеними Міжнародною організацією зі стандартизації, дасть компаніям змогу інтегрувати свої системи управління інформаційною безпекою в наявні процеси найбільш ефективно.

Ключові слова: *інформаційна безпека, інформаційний ризик, міжнародний стандарт з інформаційної безпеки.*

I. Вступ

Будь-яка діяльність підприємства супроводжується подіями, які можуть нести як позитивні можливості, так і небезпеку для підприємства. Урахування ризиків при розробці корпоративної стратегії дає змогу бути більш підготовленим до будь-яких можливих ситуацій. Керуючи ризиками результативно й ефективно, організація досягає своїх цілей з меншими витратами.

Один із видів ризиків – інформаційний – це міра інформаційної небезпеки, що характеризує ймовірність появи небезпеки та розміри пов'язаного з нею збитку для об'єкта [1].

II. Постановка завдання

Зменшення інформаційного ризику можна досягти шляхом побудови моделей оцінювання інформаційного ризику та подальшого управління ризиками. А це можливо тільки при використанні стандартів у галузі інформаційної безпеки (ІБ) та програмних продуктів.

Метою статті є аналіз міжнародного стандарту з інформаційної безпеки ISO / IEC 27001, що буде основою для побудови моделей оцінювання інформаційного ризику.

III. Результати

Для оцінювання ризиків рекомендовано використовувати стандарти, регламенти, керівництва. Насамперед, це документи міжнародних організацій із стандартизації ISO, IEC (ISO / IEC):

– ISO 17799 і 27001 (інформаційна безпека);
– ISO 17776 (нафтова і газова промисловість), 17666 (космічні системи), 14971 (медичне обладнання), 14121, 13335, 15408, 16085, 20993, 22367;
– IEC 60300-3-9, 60812, 61025, 61508-2, 61822, 62198 і Керівництво з принципів і впровадження ризик-менеджменту (ISO / TMB / WG RiskManagement);
– ISO / IEC Guide73;
– ISO / IEC Guide 51 [2].

У 1992 р. Міністерство торгівлі і промисловості Великобританії опублікувало Кодекс управління інформаційною безпекою (Code of Practice for Information Security Management). Саме цей Кодекс пізніше було покладено в основу міжнародного стандарту з інформаційної безпеки.

Міжнародний стандарт ISO / IEC 27001:2005 "Системи менеджменту інформаційної безпеки. Вимоги" встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси [7].

Система менеджменту інформаційної безпеки включає в себе важливі стандартні операційні процедури, такі як управління ризиками, управління документами, управління записами, внутрішній аудит, постійне вдосконалення [9].

У 2013 р. цей стандарт ISO 27001 був викладений у новій редакції і тепер має назву ISO 27001:2013 "Інформаційні технології – Методи безпеки – Системи менеджменту інформаційної безпеки – Вимоги" ("Information technology – Security techniques – Code of practice for information security controls"). Основна мета нового стандарту – забезпечити більш гнучкий, оптимізований підхід для ефективного управління ризиками [4; 5].

У нову редакцію було включено кілька показників безпеки, щоб забезпечити актуальність стандарту і його можливість застосування до сучасних ризиків, а саме: викрадення приватних даних, загроз, пов'язаних з використанням мобільних пристроїв та інших мережевих вразливостей [5].

Стандарт ISO 27001:2013 був модифікований з метою адаптації до нової загальної структури, що використовується в усіх стандартах на системи менеджменту, і це спрощує його інтеграцію з іншими системами менеджменту [5].

Отже, тепер завдяки новій структурі стандарту організації при впровадженні декількох стандартів з інформаційної безпеки значно зекономлять кошти, оскільки зможуть реалізовувати інтегровані політики і процедури. Найчастіше доводиться інтегрувати систему інформаційної безпеки ISO 27001:2013 з такими системами, як система менеджменту безперервності бізнесу ISO / IEC 22301, система менеджменту IT-послуг ISO / IEC 20000-1, система менеджменту якості ISO 9001 [5].

Організаціям, які сертифіковані за стандартом ISO 27001:2005, буде необхідно оновити систему менеджменту інформаційної безпеки, щоб забезпечити відповідність вимогам нової редакції стандарту. Нині Британський інститут стандартів (British Standards Institution) та інші сертифікаційні органи не опублікували план переходу на нову версію стандарту, однак існує декілька планів, які були використані в схожих ситуаціях з іншими стандартами. Перехідний період для оновлення приблизно становитиме два роки з моменту публікації нової редакції [4; 5].

У новій редакції стандарту збільшилась кількість обов'язкових положень з п'яти до семи (табл.) [9].

Таблиця

Порівняння структури двох редакцій Міжнародного стандарту ISO / IEC 27001

ISO / IEC 27001:2005	ISO / IEC 27001:2013
0. Вступ	0. Вступ
1. Галузь застосування	1. Галузь застосування
2. Нормативні посилання	2. Нормативні посилання
3. Терміни і визначення	3. Терміни і визначення
4. Система інформаційної безпеки	4. Система інформаційної безпеки
5. Зобов'язання керівництва	5. Контекст організації
6. Внутрішні аудити	6. Планування
7. Аналіз системи менеджменту	7. Підтримка
8. Удосконалення	8. Операції (експлуатація)
	9. Оцінювання (вимірювання) результативності
	10. Удосконалення

В додатку А "Цілі та механізми контролю" також збільшилась кількість розділів з 10 до 13.

Надамо перелік розділів у стандарті 2005 р.:

– Політика в галузі безпеки;
– Організація системи безпеки;
– Класифікація активів і управління;
– Безпека та персонал;
– Фізична та зовнішня безпека;
– Управління комунікаціями та операціями;
– Управління доступом до системи;
– Придбання, розробка та обслуговування інформаційних систем;
– Менеджмент інцидентів;
– Забезпечення безперервності бізнесу;
– Відповідність законодавству [9].

У редакції 2013 р.:

– було виділено такі розділи: "Криптографія" та "Відносини з постачальниками" (раніше вимоги цих розділів теж містились, але були розподілені в інших розділах і додатках);
– розділ "Управління комунікаціями та операціями" розподілений на два самостійні розділи: "Безпека комунікацій" та "Безпека операцій" [4; 9].

Оновлений стандарт ураховує інтереси всіх сторін, що взаємодіють з організацією (акціонерів, регуляторів, клієнтів, партнерів) і дає змогу визначити окремі вимоги для кожного з них.

Нова вимога стандарту стосується необхідності визначення переліку осіб (усередині й поза організацією), з якими необхідно взаємодіяти з питань, пов'язаних з управлінням ІБ. Тепер компанія повинна визначити інформацію, яку необхідно довести до відома зацікавлених осіб, а також коли, хто і як повинен це робити. З уведенням такої процедури має спроститися залучення керівництва та власників бізнес-процесів до управління ІБ, оскільки тепер вони можуть отримувати всю актуальну інформацію, що стосується функціонування системи управління ІБ [4].

У минулій версії стандарту не було чіткої структури вимог про те, як необхідно формулювати завдання і як планувати їх виконання − подібні вимоги були рознесені по різних розділах стандарту. Тепер все зібрано воєдино і разом з розділом "Моніторинг, вимірювання, аналіз та оцінка" являє собою потужний інструмент з управління ІБ в організації, який буде необхідний вищому керівництву для оцінювання поточної ситуації та планування подальших дій.

При перевірці, якщо аудитор системи менеджменту інформаційної безпеки виявляє, що хоч один з обов'язкових пунктів стандарту відсутній або неефективний, це вважається однією з основних невідповідностей, а значить, підприємство не буде

рекомендовано для видачі сертифіката або може бути його дасть змогу.

Система управління інформаційною безпекою на основі стандарту ISO 27001 дасть змогу:

– зробити більшість інформаційних активів найбільш зрозумілими для менеджменту компанії;
– виявляти основні загрози безпеки для наявних 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 й виправляти слабкі місця в системі інформаційної безпеки);
– чітко визначити особисту відповідальність;
– досягти зниження й оптимізації вартості підтримки системи безпеки;
– полегшити інтеграцію підсистеми безпеки в бізнес-процеси та інтеграцію з ISO 9001:2000;
– продемонструвати клієнтам, партнерам, власникам бізнесу свою прихильність до інформаційної безпеки;
– отримати міжнародне визнання та підвищення авторитету компанії, як на внутрішньому, так і на зовнішніх ринках;
– підкреслити прозорість і чистоту бізнесу перед законом завдяки відповідності стандарту [7].

IV. Висновки

Стандарт ISO 27001 був усесвітньо визнаний як стандарт інформаційної безпеки, якого дотримуються організації, що гарантують захист своїх інформаційних активів. Якщо в організації є сертифікат ISO 27001, то це означає, що вона пройшла перевірку і прийняла всі вимоги найвищих критеріїв управління інформаційною безпекою [6].

З 2005 р. сертифікаційний аудит на відповідність вимогам стандарту ISO / IEC 27001 пройшло понад 17 тис. компаній по всьому світу (за даними BSI). Ще більше компаній не подавали заявок на проведення сертифікаційного аудиту, але використовували стандарт як джерело кращих практик при проектуванні систем управління інформаційною безпекою [6].

Отже, нова редакція Міжнародного стандарту з інформаційної безпеки ISO / IEC 27001:2013 сприяє більшому залученню в процеси управління ІБ керівництва організації і дає інструмент, який дасть змогу ефективніше взаємодіяти топ-менеджменту та особам, відповідальним за ІБ.

Деякі вимоги стандарту стали менш суворими, що дає більшу гнучкість для компанії у виборі методик і захисних заходів. Вимоги та заходи попередньої версії були істотно оптимізовані і, відповідно, багато спірних моментів було усунено.

Гармонізація ISO / IEC 27001:2013 з усіма сучасними стандартами, випущеними Міжнародною організацією із стандартизації, дасть компаніям можливість інтегрувати свої системи управління ІБ в наявні процеси найбільш ефективно (якщо процеси побудовані на методологіях стандартів ISO).

Отже, існує безліч стандартів інформаційної безпеки. Але які б стандарти організація не застосовувала, визнавши їх найбільш придатними для себе, вигоди стандартизації очевидні − це сприятливий імідж організації, демонстрація її стабільного становища, зниження витрат, пов'язаних з обробкою інцидентів ІБ, зниження рівня ризиків ІБ, підвищення обізнаності працівників у галузі ІБ тощо.

Список використаної літератури

1. Аналитическое агентство Смыслография [Электронный ресурс]. – Режим доступа: http://www.s-graph.ru/Glossary/37/.
2. Безопасность и управление рисками [Электронный ресурс]. – Режим доступа: http://www.comizdat.com/index_.php?in=ksks_articles_id&id=567.
3. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования [Электронный ресурс]: международный стандарт. – Режим доступа: http://etr-spektr.com.ua/standarts_download/ISO-IEC_27001-2005.pdf.
4. Международный стандарт ISO / IEC 27001:2013. Взгляд в будущее индустрии ИБ [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/articles2/pravo/mezhdunarodnyy-standart-iso-iec-27001 2013.-vzglyad-v-buduschee-industrii-ib/.
5. Новая версия стандарта ISO/IEC 27001 поможет эффективнее бороться с рисками в ИТ [Электронный ресурс]. − Режим доступа: http://www.iso.org/iso/ru/home/news_index/news_archive/news.htm?refid=Ref1767.
6. Официальный сайт "Ависта консалтинг" [Электронный ресурс]. – Режим доступа: http://avista24.ru/sertifikaciya/iso_27001/.
7. Система менеджмента информационной безопасности по требованиям международного стандарта ISO/IEC 27001:2005 [Электронный ресурс]. − Режим доступа: http://www.tuev-nord.com.ua/index.php/sertsm/isoiec-27001.
8. Стандартизация в области информационной безопасности: зарубежный опыт [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/articles2/pravo/standartiz-v-oblasti-ib-zarubezhn-oput-chast-2.
9. Стандарт ISO/IEC 27001:2013 [Электронный ресурс]. – Режим доступа: http://intercert.com.ua/articles/posts/292-standart-iso-iec-27001-2013.

10. Управление информационной безопасностью ISO / IEC 27001:2013 [Электронный ресурс]. – Режим доступа: http://tms-ua.com/standarts/iso-27001-2013/.

Стаття надійшла до редакції 10.01.2014.

Сикорский Д.О. Построение процесса защиты информации на основе международного стандарта по информационной безопасности

В статье осуществлён анализ Международного стандарта по информационной безопасности ISO / IEC 27001, в частности новой редакции 2013 г. Проведено сравнение структуры двух вариантов стандарта и изложены возможности нового стандарта. Проведенный анализ является основой для построения моделей оценки информационного риска. Гармонизация ISO / IEC 27001:2013 со всеми современными стандартами, выпущенными Международной организацией по стандартизации, позволит компаниям интегрировать свои системы управления информационной безопасностью в существующие процессы наиболее эффективно.

Ключевые слова: *Информационная безопасность, информационный риск, международный стандарт по информационной безопасности.*

Sikorskyi D. Construction process of information security based on international standard for information security

The paper presents the analysis of the International Standard for Information Security ISO / IEC 27001, in particular, the new revisionof 2013.

Information Security Management Systems includes important operation procedures such as risks management, documents management, records management, internal audit, constant improvement.

The study compares the structure of the two variants of the standard and outlined possible of new standard. The analysis is the basis for constructing models of risk assessment information. Harmonization of ISO / IEC 27001:2013 with all modern standards, issued by the International Organization for Standardization, will allow companies to integrate their information security management system in existing processes more efficiently.

If the organization introduces few standards, new structure of the standard allowsto save money, because organization can implements the integration policies and procedures. There is a necessity to integrate the information security system ISO 27001:2013 with such system as business management continuity ISO / IEC 22301, management system of IT services ISO / IEC 20000-1, quality management system ISO 9001.

Some requirements have become less stringent; it gives choice flexibility of methods and protective measures. Requirements and measures of the previous version have been significantly optimized and, therefore, many contentious issues have been overcome.

Harmonization of ISO / IEC 27001:2013 with all current standards issued by the International Organization for Standardization, enables companies to integrate their information security management system in existing processes more effectively (if processes are built on the methodology of standards ISO).

So, there are many standards of information security. But the use of any standard is benefits: a good image of the organization, the demonstration its stable position and so on.

Key words: *information security, information risk, international standard for information security.*