УДК 35.004

RISK MANAGEMENT PROCESS OF INFORMATION SECURITY

D. Bilokon, I. Fedulova
National University of Food Technologies

Key words:
Information security risks
Risk management
Information security
OCTAVE information security methodology

Article history:
Received 17.09.2016
Received in revised form 23.09.2016
Accepted 21.10.2016

Corresponding author:
D.Bilokon
E-mail:
dbilokon@gmail.com

ABSTRACT

The article is devoted to the study of risk management methods of information security. The purpose of the article is to study the basic procedures, principles, functions and methodological support for analysis process and management of information security risks. The essence of OCTAVE methodology and implementation features of the mechanism of information security risk management was considered. The methodology of OCTAVE information security was analysed in the article. We commented on the need for constant systemic risk research and support of enterprise information security using the OCTAVE technique.

ПРОЦЕС УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Д.С. Білоконь, І.В. Федулова
Національний університет харчових технологій

У статті досліджено основні процедури, принципи, функції і методичне забезпечення процесу аналізу й управління ризиками інформаційної безпеки підприємства. Розглянуто сутність методології OCTAVE, особливості впровадження механізму інформаційної безпеки, проаналізовано методику управління ризиками інформаційної безпеки OCTAVE. Обґрунтовано необхідність постійного системного дослідження ризиків і підтримки інформаційної безпеки підприємства з використанням методики OCTAVE.

Ключові слова: *ризики інформаційної безпеки, управління ризиками, інформаційна безпека, захист інформації, методологія OCTAVE.*

Постановка проблеми. На сьогодні багатьом підприємствам конче необхідно володіти вмінням аналізу й управління інформаційними ризиками не тільки для отримання конкурентних переваг, а й для виживання. Проте багатьом організаціям минулого століття для успішної діяльності мистецтво

управління ризиками було зовсім не потрібне, однак дане питання сьогодні загострилось. На нашу думку, це пов'язано з швидкоплинністю часу, значним збільшенням інформаційних загроз, а також обмеженою кількістю технологій і стандартів у минулих десятиліттях порівняно з сьогоденням. Сучасний світ швидко змінюється, для нового інформаційного століття характерні неуявні досі загрози та кризи. Щоденно реєструється величезна кількість мережевих атак і внутрішніх інцидентів інформаційної безпеки. Варто зазначити, що скоординовані атаки на об'єкти інфраструктури (електростанції, телекомунікаційні вузли, системи водо, тепло-, газопостачання) можуть стати причиною глобальної катастрофи, наслідки якої важко уявити.

Аналіз останніх досліджень і публікацій. Відповідно до сучасних міжнародних стандартів, ризик — це стан впливу чинників невизначеності на досягання мети [12]. Реалізація ризику призводить до відхилення фактичних результатів діяльності від запланованих. Ризик — це діяльність, пов'язана з подоланням невизначеності в ситуації неминучого вибору, в процесі якої існує можливість кількісно і якісно оцінити ймовірність досягнення передбачуваного результату, невдачі і відхилення від мети.

Сутність сучасної організації пов'язана з використанням існуючих інформаційно-комунікаційних технологій та інших інтелектуальних активів для здійснення господарської діяльності й досягнення цілей. Ця діяльність, як правило, пов'язана з невизначеністю та ризиками. На сьогодні не існує механізмів, що дозволяють повністю захистити організацію від загроз і ризиків, але ризики можна істотно знизити шляхом впровадження системи управління ризиками інформаційної безпеки.

Інформаційна безпека включає три складові управління: вимоги до управління, політику управління ризиками та механізми ідентифікації, аналіз та оцінку ризику. Вимоги визначаються тими цілями, які ставлять перед собою підприємства для забезпечення безпеки. Політика управління інформаційною безпекою визначається її вагомістю і значенням для ефективної господарської діяльності підприємства. Політика має визначити напрями і заходи досягнення цілей. Організаційно-економічний механізм управління підприємством визначає особливості формування політики. В механізмі управління важливим є визначення інструментів, методів, процедур та інших засобів обґрунтування рішень у процесі забезпечення інформаційної безпеки з визначенням та ідентифікацією всіх видів ризиків.

Методи оцінки ризику поділяються на кількісні і якісні, найбільш ефективним є поєднання цих двох підходів в інтегрованій системі управління ризиками інформаційної безпеки підприємства.

Світова практика пропонує такі найбільш поширені на даний час методики оцінки ризиків інформаційної безпеки:

1. CRAMM. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Метод є універсальним, його можна застосовувати як для урядового, так і для комерційного сектору. Грамотне використання методу CRAMM дозволяє отримувати високі результати, серед яких можливість економічного обґрунтування витрат організації на забезпечення інформаційної безпеки й безперервності

бізнесу. Цей метод, незважаючи на значну універсальність і функціональність, має такі недоліки, як необхідність спеціальної підготовки користувачів і значна вартість ліцензії [8].

2. IT-Grundschutz. IT-Grundschutz пропонує спосіб для створення системи управління інформаційною безпекою, яка включає в себе як загальні рекомендації щодо забезпечення безпеки IT, так і допоміжні технічні рекомендації для досягнення необхідного рівня IT безпеки для конкретного домену. У методі IT-Grundschutz представлені каталоги: 1) модулі; 2) каталоги загроз; 3) каталоги захисту. Дана методика має більш рекомендаційний, теоретичний характер, ніж практичний [11].

3. NIST. Передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози. Методика охоплює широке коло завдань, що пов'язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику інформаційної безпеки відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. Оцінювання ризиків проводиться за трирівневою шкалою, що істотно обмежує можливості методики загалом [4].

Як бачимо, в розглянутих нами методиках існують певні обмеження і суттєві недоліки та складнощі із застосування на практиці. Методика управління ризиками інформаційної безпеки OCTAVE загальнодоступна й універсальна. Цю методику широко використовують у всьому світі, оцінюючи ризики інформаційної безпеки та впроваджуючи процеси управління ризиками в організації загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру й галузі діяльності [2].

Мета статті полягає в дослідженні основних процедур, принципів, функцій і методичного забезпечення процесу аналізу й управління ризиками інформаційної безпеки.

Виклад основних результатів дослідження. Аналізу інформаційних ризиків у нашій країні не приділялося належної уваги до прийняття Доктрини інформаційної безпеки України в 2009 р., тому на сьогодні ця тема активно досліджується і впроваджується в практику спеціалістами сфери інформаційної безпеки. У той же час на особливу увагу заслуговують питання практичного застосування існуючих методик аналізу ризиків та їх вдосконалення [5].

Також в останні роки здійснюється розробка і впровадження в систему інформаційної безпеки підприємств міжнародних стандартів серії 27000, що визначають вимоги до системи менеджменту інформаційної безпеки.

Інформаційне забезпечення функціонування ризик-менеджменту складається з різного роду і виду інформації: статистичної, економічної, комерційної, фінансової тощо. Ця інформація включає обізнаність про ймовірність того чи іншого страхового випадку, страхової події, наявність і величину попиту на товари, на капітал, фінансової стійкості та платоспроможності клієнтів, партнерів, конкурентів, ціни, курси й тарифи, в тому числі на послуги, дивіденди і відсотки тощо.

Великою популярністю останнім часом користується методологія аналізу ризиків інформаційної безпеки OCTAVE, розроблена інститутом Software Engineering Institute (SEI) при університеті Карнегі Меллона (Carnegie Mellon University). Ця методологія передбачає здійснення процесу аналізу ризиків інформаційної безпеки лише працівниками підприємства без залучення зовнішніх консультантів через те, що такі працівники краще розуміють потреби підприємства і властиві йому ризики [10].

За цією методикою відбувається розробка профілю загроз, виявлення вразливостей в інформаційній безпеці і розроблення стратегії забезпечення безпеки. Для кожного джерела загроз будується дерево варіантів, яке наочно показує вигляд загрози і шляхи її усунення. При оцінці ризиків інформаційної безпеки формується шкала за трьома позиціями: високий, середній і низький рівень ризику, встановлюється можливий фінансовий збиток. Основною перевагою даної методики є: загальнодоступність і безкоштовність, швидке впровадження, можливість застосування для організацій різного розміру та галузей зайнятості, наявність комерційних програмних продуктів, що реалізують положення методики, високий рівень гнучкості [1]. До недоліків потрібно віднести те, що дана методика не дає кількісної оцінки ризиків.

OCTAVE широко використовують у всьому світі для оцінки ризиків інформаційної безпеки та впровадження процесів управління ризиками в підприємстві в цілому.

Методика має три модифікації, які розраховані на організації різного розміру:

- методологія оцінки ризиків OCTAVE Method застосовується для достатньо великих підприємств (від 300 осіб і більше);
- спрощена методологія оцінки ризиків OCTAVE-S, орієнтована на підприємства середнього розміру (не більше 100 осіб);
- методологія оцінки ризиків OCTAVE Allegro, яка може застосовуватися консультантами на індивідуальній основі без широкого залучення в процес оцінки ризиків співробітників організації [3]

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops) (рис. 1).

Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи [6].

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять у собі інвентаризацію й оцінку цінності активів, ідентифікацію застосовних вимог законодавства й нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів для підтримки режиму інформаційної безпеки. На другому етапі проводиться технічний аналіз вразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних вразливостей компанії й оцінювання їх величини. На третьому етапі виконується оцінка й оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди

внаслідок реалізації загроз інформаційної безпеки з використанням вразливостей, які ідентифіковано на попередніх етапах, визначення стратегії інформаційної безпеки, а також вибір варіантів і прийняття рішень з оброблення ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз інформаційної безпеки.

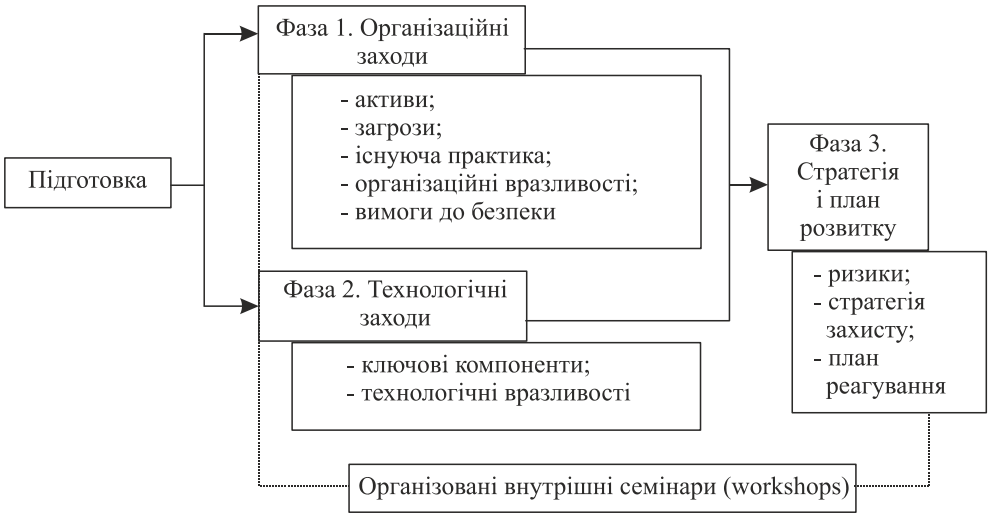

Рис. 1. Послідовність трьох складових фаз методу OCTAVE [3]

Для аналізу ризиків у методиці OCTAVE пропонується підхід з восьми кроків, об'єднаних в чотири етапи (рис. 2).

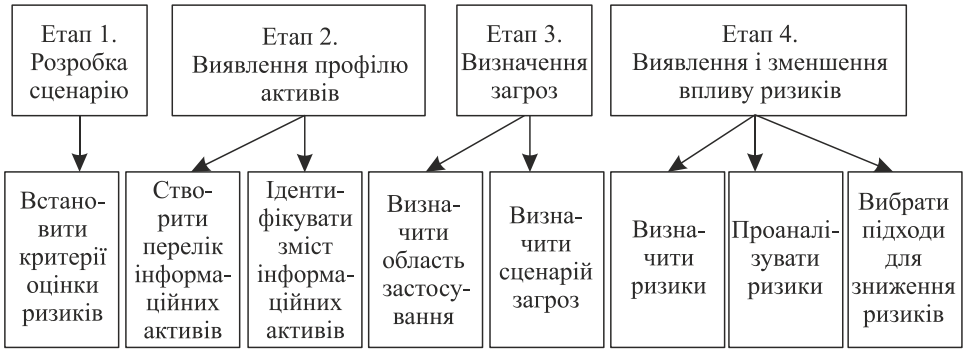

Рис. 2. Етапи аналізу ризиків за методикою OCTAVE,
складено автором на основі [1, 2, 3]

Розглянемо загальний алгоритм дій щодо аналізу ризиків, заснований на методиці OCTAVE, а також рекомендації щодо впровадження в систему менеджменту інформаційної безпеки організації оцінки ризиків на постійній основі і моніторингу ризиків інформаційної безпеки.

На кроці 1 необхідно визначити критерії оцінки ризиків інформаційної безпеки, тобто сукупність якісних показників, яка дозволить встановити значення оцінки ризику і наслідки реалізації ризику. Без введення таких

критеріїв неможливо оцінити залежність організації від тих чи інших ризиків. Такими критеріями можуть бути використані вимоги безпеки, застосовувані на підприємстві, рівень інвестицій і витрат на інформаційну безпеку, стратегічна цінність і критичність порушених інформаційних активів тощо. Критерії оцінки ризиків повинні відображати усвідомлення інформаційних ризиків, які існують у сфері діяльності організації. Критерії встановлюють діапазон наслідків реалізації ризику: низькі, середні і високі.

Крок 2 починається зі складання переліку інформаційних активів і визначення їх профілю. Профіль — це інформація, яка описувала актив його унікальними особливостями, якостями, характеристиками, вартістю. Профілювання дозволяє чітко визначити «кордони» активу і вимоги безпеки до нього. Профіль створюється для кожного активу й описується на окремому аркуші. Профіль активу являє собою вхідні дані для наступних кроків і є основою для виявлення загроз і ризиків.

Крок 3. Інформаційні активи можуть зберігатися не тільки в самій організації, але і поза її межами. Наприклад, організація може допускати до обслуговування своєї інфраструктури інші організації-постачальники послуг. Ризик може міститися в самому факті зберігання, передачі або обробки активу. Це порушує захист інформаційного активу. Ще більшу загрозу несе залучення таким постачальником послуг субпідрядників, про які власник активу може і не знати. Таким чином, для отримання адекватного профілю активу важливо визначити всі місця зберігання, передачі й обробки активу — контейнери, а також місце знаходження в зоні управління організації.

На кроці 3 створюється карта активу, де вказуються всі місця його зберігання, передачі і обробки, які можуть стати точками уразливості або, навпаки, точками, які можна повністю контролювати, гарантуючи захищеність активу. Місцем зберігання активу може бути технічний засіб, програмне забезпечення, паперовий носій або співробітник організації.

На кроці 4 виявляються проблемні області в інформаційній безпеці підприємства. Метою кроку є оперативне визначення тих загроз, які відразу очевидні для аналітика.

Крок 5: на основі виявлених проблемних областей, складаються сценарії загроз, які візуально ефективно представляти у вигляді дерева, де з метою більш надійного розгляду загроз кожна гілка розглядається для кожного інформаційного активу. Для полегшення визначення сценарію загроз по кожній гілці необхідно використовувати опитувальні анкети. Цей крок також дозволяє врахувати ймовірності реалізації загроз, що допомагає на більш пізніх етапах розробити заходи щодо зниження ризику. Як правило, в цьому випадку використовується якісна шкала, і вводяться три рівні ймовірності реалізації загрози: висока, середня і низька.

На кроці 6, після визначення загроз і виявлення наслідків їх реалізації, визначають ризики інформаційної безпеки. Необхідно визначити, як саме ризик буде впливати на організацію або актив, при цьому ризик визначається для кожного активу, щоб оцінити його критичність для організації або самого активу.

На кроці 7 визначається кількісна міра шкоди, яка буде завдана організації при реалізації загрози. Це відносна оцінка, яка дозволяє розставити ризики за їх пріоритетом. Наприклад, якщо для компанії найбільш важлива її репутація на ринку, то передусім треба пом'якшувати ризики саме цієї проблемної області. Робочі листи й опитувальні анкети, які застосовуються в процесі аналізу ризиків, а також розгорнута інструкція щодо впровадження і застосування OCTAVE, містяться в англомовному описі методики «Introducing OCTAVE Allegro: Improving the Inform ation Risk Assessment Process»,_представленому на сайті www.cert.org.

На заключному етапі вибираються заходи для обробки певних ризиків з урахуванням їх пріоритету для організації. Рішення про прийняття, зменшення або відкладення ризику ґрунтується на ряді факторів, основними з яких є величина впливу ризику і ймовірність його реалізації. Якщо ризик може серйозно впливати на організацію, але при цьому малоймовірний, то, можливо, він не вартий пом'якшення. Рішення про те, які ризики пом'якшувати, а які ні, повинні приймати аналітики і/або керівництво організації.

Вибір стратегії пом'якшення ризику — складне завдання і його вирішення вимагає взаємодії з іншими фахівцями організації. Обрана стратегія повинна гарантувати захист активів відповідно до критеріїв безпеки. Необхідно враховувати витрати на пом'якшення ризику, тому що вони, як мінімум, не повинні перевищувати вартість активу [10].

Висновки

Процес впливу суб'єкта на об'єкт управління, тобто сам процес управління, може здійснюватися тільки за умови обміну певної інформації між керуючою і керованою підсистемами. Процес управління незалежно від його конкретного змісту завжди передбачає отримання, передачу, переробку і використання інформації. У ризик-менеджменті отримання надійної і достатньої в даних умовах інформації відіграє головну роль, тому що дозволяє прийняти конкретне рішення щодо дій в умовах ризику. Будь-яке рішення ґрунтується на інформації. Важливе значення має якість, надійність і вчасність інформації. Якість інформації має оцінюватися при її отриманні, а не при передачі. Інформація старіє швидко, тому її слід використовувати оперативно.

Оцінку ризиків інформаційної безпеки слід проводити на постійній основі, при цьому проводити її рекомендується не менше, ніж раз на рік. Ризики інформаційної безпеки потрібно регулярно відстежувати, для чого необхідно впроваджувати систему моніторингу ризиків. Це пов'язано зі швидким розвитком інформаційних технологій і, як наслідок, з виникненням нових ризиків інформаційної безпеки, можливим старінням і виключенням деяких раніше прийнятих ризиків або втрати ефективності заходів, прийнятих раніше.

Література

1. *Christopher J.* Alberts. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0 / Christopher J. Alberts, Sandra G. Behrens, Sandra G. Behrens, Sandra G. Behrens. — Pitsburg: Carnegie Mellon University, 1999. — 72 p.

2. Introducing OCTAVE Allegro: Improving the Information Risk Assessment Process. — Software Engineering Institute, 2007. — 154 c.

3. Software Engineering Institute Carnegie Mellon University [Електронний ресурс]. — Режим доступу: http://www.cert.org.

4. *Swanson M.* NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems / M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, D. Lynes. — 2010. — 149 p.

5. *Балашов П.А.* Оценка рисков информационной безопасности на основе нечеткой логики: учебное пособие / П.А. Балашов, В.К. Безгузиков, Р.И. Кислов. — Москва: Научная литература, 2009. — С. 165.

6. *Баранова Е.К.* Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Сер. 3: Образовательные ресурсы и технологии. — 2015. — № 1(9). — С. 73—79.

7. *Баранова Е.К.* Управление инцидентами информационной безопасности. Проблемы информационной безопасности / Е.К. Баранова, Г.Б. Зубровский // Труды I Международной научно-практической конференции «Проблемы информационной безопасности». — Гурзуф, Крымский федеральный университет им. В.И. Вернадского, 2015. — С. 27—33.

8. *Гарасим Ю.Р.* Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем / Ю.Р. Гарасим, В.А. Ромака, М.М. Рибій // Вісник Національного університету «Львівська політехніка» «Автоматика, вимірювання та керування». — 2013. — № 756. — С. 105—123.

9. *Куканова Н.А.* Актуальность задачи — обеспечение информационной безопасности для бизнеса: монография / Н.А. Куканова. — Киев: Бизнесинформ, 2010. — С. 136.

10 Методологии управления ИТ-рисками. — Москва: Информационный ресурс, 2010. — 103 с.

11. Методология OCTAVE для оценки информационных рисков. — Москва: Информационный ресурс, 2005. — С. 25.

12. *Мохор В.* Спроба локалізації ISO GUIDE 73:2009 «RISK MANAGEMENT — VOCABULARY» / В. Мохор, О. Богданов, О. Крук, В. Цуркан // Ukrainian Scientific Journal of Information Security. — 2012. — № 2 (18). — С.12—22.

ПРОЦЕСС УПРАВЛЕНИЯМИ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.С. Белоконь, И.В. Федулова
Национальный университет пищевых технологий

В статье исследованы основные процедуры, принципы, функции и методическое обеспечение процесса анализа и управления рисками информационной безопасности предприятия. Рассмотрены сущность методологии OCTAVE и особенности внедрения механизма информационной безопасности, проанализирована методика управления рисками информационной безопасности OCTAVE. Обоснована необходимость постоянного системного исследования рисков и поддержки информационной безопасности предприятия с использованием методики OCTAVE.

Ключевые слова: *риски информационной безопасности, управление рисками, информационная безопасность, защита информации, методология OCTAVE.*