УДК 004.056.5(045)

Чунарьова А.В., к.т.н.

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РЕСУРСІВ НА БАЗІ СИСТЕМИ ОЦІНКИ РИЗИКІВ

Інститут комп'ютерних інформаційних технологій НАУ,

chunariova@gmail.com

Проведено аналіз основних положень системи менеджменту ризиків інформаційної безпеки та його основних етапів проведення. На основі аналізу основних складових системи менеджменту ризику інформаційної безпеки розроблена узагальнена структурна схема процесу оцінки ризиків

Ключові слова: система оцінки ризиків, інформаційна безпека, ризики, загроза, уразливості

Вступ

Процес управління ризиками безпеки є комбінованим підходом, що об'єднує елементи кількісного та якісного методів аналізу. Об'єднуючи простоту якісного методу та детальність кількісного, керівництво пропонує унікальний процес управління ризиками безпеки, що поєднує ефективність та зручність використання та покликаний забезпечити розуміння кожного кроку оцінки всіма зацікавленими особами. Якісний підхід значно простіший, ніж традиційне кількісне управління ризиками; він зменшує протидію на етапах аналізу ризику та підтримки ухвалення рішень, дозволяє швидше знайти задовільне рішення та легко забезпечувати підтримку впродовж всього процесу.

Постановка задачі

На сьогоднішній день процес управлінням ризиками організації є невід'ємною частиною процедури системи менеджменту інформаційної безпеки. Під поняттям управління ризиками будемо розуміти процеси, пов'язані з ідентифікацією, аналізом ризиків та прийняттям рішень по їх мінімізації. На даний час процес управління ризиками інформаційної безпеки зазвичай включає виконання наступних обов'язкових процедур:

1. Планування управління ризиками – вибір підходів і планування діяльності з управління ризиками.

2. Ідентифікація ризиків – визначення ризиків, здатних негативно впливати на критичні інформаційні ресурси, і документування їх характеристик.

3. Якісна оцінка ризиків – якісний аналіз ризиків і умов їх виникнення з метою визначення їх впливу ні інформаційну систему.

4. Кількісна оцінка – кількісний аналіз ймовірності виникнення та впливу наслідків ризиків.

5. Планування реагування на ризики – визначення процедур і методів з ослаблення негативних наслідків ризикових подій та використання можливих переваг.

6. Моніторинг та контроль ризиків – моніторинг ризиків, визначення залишаються ризиків, виконання плану управління ризиками проекту і оцінка ефективності дій з мінімізації ризиків.

Проведення аналізу інформаційних ризиків здійснюється на основі результатів комплексного обстеження (аудиту) інформаційної безпеки. У якості бази використовуються відомі західні методики та стандарти серії ISO 27000, а також із застосуванням спеціалізованого інструментарію [1-3].

Метою даних досліджень є аналіз основних складових системи менеджменту ризику та розробка узагальненої структурної схеми процесу оцінки ризиків інформаційної безпеки.

Основні положення системи менеджменту ризиків інформаційної безпеки

Менеджмент ризику інформаційної безпеки організації має бути безперерв-

ним процесом. В рамках даного процесу слід проводити оцінку і обробку ризиків, використовуючи для реалізації рекомендації і планів обробки ризиків. До прийняття рішення про те, що і коли повинно бути зроблено для зниження ризику до прийнятного рівня.

Менеджмент ризику інформаційної безпеки має сприяти: ідентифікації ризиків; оцінці ризиків, виходячи з наслідків їх реалізації для бізнесу та ймовірності їх виникнення; усвідомлення і інформування про ймовірність і наслідки ризиків; встановлення пріоритетів в рамках обробки ризиків; встановлення пріоритетів заходів щодо зниження мають місце ризиків; залучення третіх сторін до прийняття рішень про менеджмент ризику та підтримання їх інформованості про стан менеджменту ризику; ефективності проведеного моніторингу обробки ризиків; проведення регулярного моніторингу та перегляду процесу менеджменту ризику; збору інформації для вдосконалення менеджменту ризику; підготовці менеджерів і персоналу з питань ризиків і необхідних дій, що вживаються для їх зменшення.Процес менеджменту ризику та його оцінка може бути застосований до всієї організації, до будь-якої окремої частини організації (наприклад, підрозділу, філії, служби), до будь-якої інформаційної системи, до наявних. плановаим або специфічним аспектам управління (наприклад, до планування безперервності бізнесу). Якісна процедура управління ризиками повинна базуватися на наступних керівних принципах, а саме: комплексності, системності, інформативності, інтегрованості, прогнозованості. Виходячи о сформованих принципів виділимо основні функції системи управління ризиками: ідентифікації, планування, оцінка, обробка, контроль, документування. Переваги використання системи управління ризиками: проведення ідентифікації інформаційних активів та їх цінності; ідентифікація загроз і вразливостей інформаційної безпеки; оцінка і аналіз ризиків; планування засобів і методів мінімізації інформаційних ризиків згідно міжнародних стандартів серії ISO; впровадження засобів контролю та моніторинг; аудит та контроль інформаційних ризиків [1,4,5]. На рис. 1 показано чотири етапи процесу управління ризиками безпеки:

- Оцінка ризику. Виявлення та пріоритезация ризиків для бізнесу.

- Підтримка ухвалення рішень**.** Пошук та оцінка рішень для контролю на основі визначених раніше правил аналізу витрат.

- Реалізація контролю**.** Розгортання та використання рішень для контролю, що знижують ризик для організації.

- Оцінка ефективності**.** Аналіз ефективності процесу управління ризиками та перевірка того, чи забезпечують елементи контролю належний рівень безпеки.

Першим етапом є оцінка ризику, що поєднує можливості якісного та кількісного підходу. При цьому якісний підхід використовується для швидкого впорядковування переліку всіх ризиків безпеки, а кількісний підхід дозволяє надалі виконати глибший аналіз найбільш істотних ризиків, виявлених на цьому етапі. Це дає можливість сформувати відносно невеликий перелік основних ризиків, що вимагають глибокого вивчення. Аналіз ризиків може бути виконаний з різним ступенем деталізації в залежності від критичності ресурсів інформаційного об’єкту, відомих вразливостей і попередніх інцидентів інформаційної безпеки [2-6]. Даний перелік використовується на наступному етапі (етапі підтримки ухвалення рішень), в ході якого пропонуються та оцінюються рішення для контролю. Надалі кращі рішення представляються організаційному відділу з забезпечення безпеки як рекомендації по мінімізації ризику.

Рис. 1. Етапи процесу управління ризиками безпеки інформаційного об'єкту

Даний перелік використовується на наступному етапі (етапі підтримки ухвалення рішень), в ході якого пропонуються та оцінюються рішення для контролю. Надалі кращі рішення представляються організаційному відділу з забезпечення безпеки як рекомендації по мінімізації ризику.

Третій етап називається етапом реалізації контролю. На цьому етапі особи, відповідальні за мінімізацію ризику, здійснюють фактичне вибір та впровадження вибраних рішень для контролю.

Четвертий етап, етап оцінки ефективності, дозволяє перевіряти, чи забезпечують елементи контролю належний рівень безпеки, та відстежувати зміни в середовищі (наприклад, додавання нових застосувань та поява нових загроз), які здатні змінити профіль ризику організації. Процес управління ризиками безпеки – безперервний процес, цей цикл повторюється при кожній новій оцінці ризику. Частота повторення даного циклу залежить від масштабу організації. Багато фахівців вважають, що якщо в організації постійно виконується проактивний моніторинг нових вразливостей, загроз та активів, даний цикл досить повторювати один раз на рік.

Процедура оцінка ризиків інформаційної безпеки

Аналіз ризиків інформаційної безпеки здійснюється за допомогою побудови моделі інформаційної системи організації. Розглядаючи засоби захисту ресурсів, взаємозв'язок інформаційних ресурсів між собою, вплив прав доступу груп користувачів, організаційні заходи, модель оцінки ризиків досліджує захищеність кожного виду інформації.

У загальному випадку процедура менеджменту ризиків інформаційної безпеки включає наступні основні дії:

1. Детальна класифікації інформаційних ресурсів.

2. Перелік всіх уразливостей та загроз по відношенню до інформації, які стали причиною отриманого значення ризику.

3. Визначення ризику для кожного цінного ресурсу організації.

4. Визначення ризику для ресурсів після вжиття контрзаходів (залишковий ризик).

5. Оцінка ефективності використаних контрзаходів з ціллю мінімізації ризику.

6. Моніторинг та переоцінка ризику інформаційної безпеки.

Оцінка ризику кількісно або якісно характеризує ризики і дає можливість керівникам призначати для них пріоритети відповідно до усвідомлюваної ними серйозністю або іншими встановленими критеріями.

Процес оцінки ризику складається з: аналізу ризику, що включає ідентифікацію ризику та встановлення значення ризику та оцінки ризику. В процесі оцінки ризику встановлюється цінність інформаційних активів, виявляються потенційні загрози та уразливості, які існують або можуть існувати, визначаються існуючі заходи і засоби контролю і управління та їх вплив на ідентифіковані ризики, визначаються можливі наслідки і нарешті, призначаються пріоритети встановленим ризикам, а також здійснюється їх ранжування за критеріями оцінки ризику.

Для того, щоб якісно оцінити ризик по відношенню до інформації, та прийняти міри та засоби по їх мінімізації необхідно проаналізувати захищеність і архітектуру побудови інформаційної системи та визначити всіх критичні активи. Першочергово власнику інформаційної системи потрібно спочатку описати архітектуру своєї мережі: всі ресурси, на яких зберігається цінна інформація; всі мережеві групи, в яких знаходяться ресурси системи (тобто фізичні зв'язку ресурсів один з одним); відділи, до яких відносяться ресурси; види цінної інформації; шкоду для кожного виду цінної інформації за трьома видами загроз; бізнес-процеси та інформація, яка в них бере участь; групи користувачів, які мають доступ до цінної інформації; клас групи користувачів; доступ групи користувачів до інформації; характеристики цього доступу (вид і права); засоби захисту інформації; засоби захисту робочого місця групи користувачів.

Визначення активів слід проводити з відповідним ступенем деталізації, що забезпечує інформацію, достатню для оцінки ризику. Ступінь деталізації, яка використовується при визначенні активів, впливає на загальний обсяг інформації, зібраної під часової оцінки ризику. Ця інформація може бути більш деталізована при подальших ітераціях оцінки ризику.

Не менш важливим етап оцінки ризиків є процедура визначення уразливостей та загроз інформаційним активам. Необхідно виявити уразливості, які можуть бути використані загрозами для реалізації неправомірних дій по відношенню інформаційних активів організації. Загроза може заподіяти шкоду важливим активам організації, таким як інформація, процеси і системи. Загрози можуть виникати в результаті природних явищ або дій людей, вони можуть бути випадковими або навмисними. Повинні бути встановлені і випадкові, і навмисні джерела загроз.

Уразливості повинні бути виявлені в наступних областях по відношенню до інформаційного об’єкту, де циркулює критична інформація:організація робіт по створенню та експлуатації захищеної інформаційної системи; процеси та процедури; робота з персоналом; фізичне та технологічне середовище; конфігурація інформаційної системи; апаратні засоби, програмне забезпечення, апаратура зв'язку, комутаційне та мережеве обладнання.

Наявність уразливості саме по собі не завдає шкоди, оскільки необхідна наявність певної загрози, яка зможе скористатися нею для реалізації процедури порушення цілісності, конфіденційності та доступності інформації. Для уразливості, відповідно до якої не відповідає певна загроза, може не знадобитися впровадження засоби контролю і управління, але вона повинна усвідомлюватися і піддаватися моніторингу на предмет змін. Слід зазначити, що невірно реалізований засіб контролю та управління стану інформаційної безпеки саме може стати уразливістю інформаційної системи. Заходи і засоби ко-

нтролю і управління можуть бути ефективними або неефективними в залежності від середовища, в якому вони функціонують.

Уразливості повинні бути пов'язані з властивостями активу. При класифікацій уразливостей необхідно враховувати ті уразливості, які виникають з різних джерел, наприклад ті, які є зовнішніми або внутрішніми по відношенню до інформаційного активу.

Далі аналіз ризику виконується з різним ступенем деталізації в залежності від критичності активів, відомих уразливостей і інцидентів, що стосуються організації. Методологія встановлення значення ризику може бути якісною, кількісної, або комбінованою. На практиці встановлення якісного значення часто використовується спочатку для отримання загальних відомостей про рівень ризику і виявлення основних значень ризиків. Пізніше може виникнути необхідність у здійсненні більш специфічного встановлення кількісного аналізу основних значень ризиків, оскільки зазвичай виконання якісного аналізу в порівнянні з кількісним є менш складним і витратним.

Для встановлення якісного значення використовується шкала кваліфікації атрибутів, за допомогою якої описуються величини можливих наслідків (наприклад низький, середній і високий) та ймовірності виникнення цих наслідків від реалізації загроз по відношенню до інформаційного активу.

Для встановлення кількісної оцінки використовується шкала з числовими значеннями як наслідків, так і ймовірності. із застосуванням даних з різних джерел. Якість аналізу залежить від точності і повноти числових значень і від обґрунтованості моделей. В більшості випадків для встановлення кількісного значення використовуються фактичні дані за минулий період. Перевага полягає в тому, що встановлення кількісного значення може бути прямо пов'язане з цілями інформаційної безпеки та проблемами організації. Спосіб вираження наслідків ризику та ймовірності його виникнення, а також способи їх комбінування для одержання інформації про рівень ризику змінюються в залежності від виду ризику і цілі, для досягнення якої повинні використовуватися вихідні дані оцінки ризику [3,7,8].

Після проведення процедури оцінки ризиків вибираються критерії оцінки ризиків. Критерії оцінки ризику, що використовуються для прийняття рішень на етапі оцінці ризиків, повинні узгоджуватися з визначеним зовнішнім і внутрішнім контекстом менеджменту ризику інформаційної безпеки і враховувати цілі організації. Рішення, пов'язані з оцінкою ризику, зазвичай ґрунтуються на прийнятному рівні ризику. Однак також повинні враховуватися наслідки, ймовірність, ступінь впевненості при ідентифікації і аналізі ризику. Сукупність безлічі ризиків низького і середнього рівня в підсумку може мати результатом загальний ризик більш високого рівня.

При оцінці ризиків необхідно враховувати: властивості інформаційної безпеки (конфіденційність, цілісність та доступність); значимість бізнес-процесу або діяльності, які підтримуються конкретним активом або сукупністю активів, якщо процес визначений як має низьку значимість, пов'язаним з ним ризиків потрібно приділяти менше уваги, ніж ризикам, що впливає на більш важливі процеси або діяльність.

Узагальнена схема процедури оцінки ризиків, як невід'ємної складової системи менеджменту ризику інформаційної безпеки представлена на рис.1

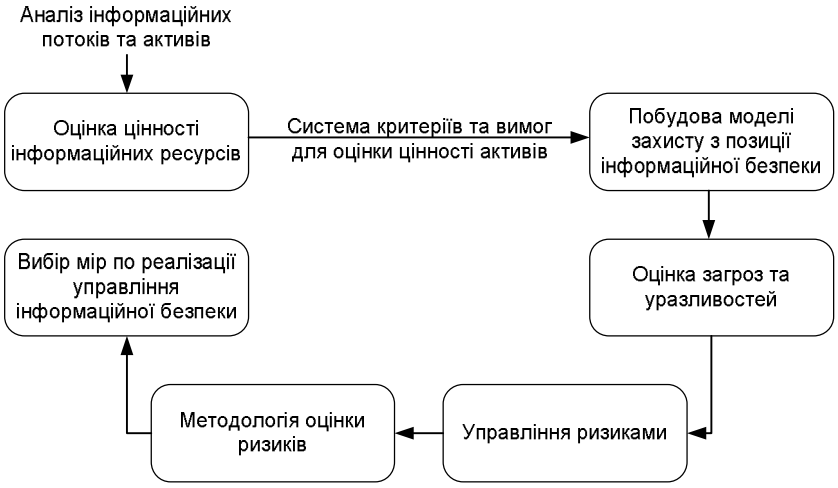

Рис.1. Структурна схема процесу оцінки ризику

Висновки

На основі проведеного аналізу основних складових системи менеджменту ризику інформаційної безпеки розроблена узагальнена структурна схема процесу оцінки ризиків. Доведено, що процес управління ризику дозволяє отримати необхідну інформацію про структуру, властивості інформаційного об'єкту і наявні ризики та вибрати механізми по мінімізації ризиків. Цей підхід є основою для побудови ефективної та коректної системи захисту.

Список література

1. Information Security Management – Specification With Guidance for Use: ISO/IEC 27001:2005.

2. Information technology – Security techniques – Code of practice for information security management : ISO/IEC 27002: 2005.

3. Information technology – Security techniques – Information security risk Magement : ISO/IEC 27005: 2008.

4. Чунарьова А.В. Система управління інформаційною безпекою підприємства / А.В.Чунарьова, А.В.Чунарьов // Nastoleni moderni vedy-2011: VII mezinarodni vedecko-prakticka confe-rence, 27.09-05.10.2011. – Praha: Publishing House «Education Science», 2011. – Dil. 11. – P. 41-44.

5. Чунарьова А.В. Концепція безпеки інформаційних ресурсів на базі системи оцінки ризиків / А.В.Чунарьова, А.В.Чунарьов // Aktuálni vymozenosti védy-2011: VII mezinarodni vedecko-prakticka conference, 27.06-05.07.2011. – Praha: Publishing House «Education Science», 2011. – Dil. 20. – P.68-72.

6. Чунарьова А.В. Оцінка ризиків сучасних корпоративних мереж / А.В.Чунарьова, А.В.Чунарьов // Ключови въпроси в съвременната наука – 2012: VII международна научна практична конф. 17 - 25 април 2012 г. – София: «Бял Град-БГ» ОДД, 2012. – Т. 30. – P.72-76.

7. Чунарьова А.В. Управління інформаційною безпекою на базі міжнародних стандартів серії ISO / А.В.Чунарьова, О.В.Фролов, О.В.Матвійчук-Юдіна // Наукоємні технології: науково-технічна конференція студентів та молодих учених, 12-16 листопада 2012 р., Київ. – К.: НАУ, 2013.

8. Чунарьова А.В. Система управління інформаційною безпекою на базі міжнародних стандартів серії ISO / А.В.Чунарьова, А.В.Чунарьов // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: науково-технічний збірник. – К.: НТУУ “КПІ”, 2012. – № 2(24). – С. 48-52.

Статтю подано до редакції 25.03.2014