УДК 004.02+004.03+004.05+005.93

Є.С. РОДІН

ПРОЦЕСНІ ПІДХОДИ ДО МОДЕЛЮВАННЯ У СФЕРІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Розкрито особливості роботи найбільш поширених моделей оцінювання ризиків інформаційної безпеки в розподілених інформаційних системах. Проаналізовано процесні підходи викладених методологій та підходи до формалізації результатів оцінювання ризиків інформаційної безпеки. Вказано на недосконалості описаних методологій і запропоновано принципи побудови більш функціональних та математично обґрунтованих моделей управління ризиками інформаційної безпеки.*
Ключові слова: *інформаційний ризик, процесна модель, інформаційна безпека, оцінка ризику.*

Аннотация. *Раскрыты особенности работы наиболее распространенных моделей оценки рисков информационной безопасности в распределенных информационных системах. Проанализированы процессные подходы изложенных методологий и подходы к формализации результатов оценки рисков информационной безопасности. Отмечено несовершенство описанных методологий и предложены принципы построения более функциональных и математически обоснованных моделей управления рисками информационной безопасности.*
Ключевые слова: *информационный риск, процессная модель, информационная безопасность, оценка риска.*

Abstract. *Working peculiarities of the most common models for information security risk assessment in distributed information systems were revealed. The analysis process approaches of outlined methodologies and approaches to the results formalization of information security risk assessment were analized. It was pointed out the imperfections of described methodologies; the principles of more functionally and mathematically based models of risk management information security were proposed.*
Keywords: *information risk, process model, information security, risk assessment.*

1. Вступ

Інформаційні системи розвиваються неймовірними темпами, перетворюються на розподілені системи з безліччю об’єктів, суб’єктів, з різноманітними інформаційними потоками. Наслідком ускладнення інформаційних систем є зростання множини факторів, що впливають на інформаційну безпеку, поява нових процесів, станів і варіантів поведінки в системах та поза їх межами. Тому при створенні надійних, гнучких систем захисту особливої актуальності набуває моделювання.

Одна з головних цілей моделювання в галузі інформаційної безпеки (ІБ) − побудова моделі, яка б враховувала найбільшу кількість впливових факторів і дозволяла розраховувати ймовірність виникнення вразливості та реалізації загрози, обчислити час реалізації загрози і можливі збитки, визначити ефективність впровадження засобів захисту та ступінь захищеності системи. Моделювання та отримання вищевказаних показників дозволить приймати рішення щодо ІБ системи, тобто управляти ризиками інформаційної безпеки.

Ключовою моделлю, використовуваною у сфері управління ризиками інформаційної безпеки (УРІБ), є процесна модель, що знайшла відображення в усіх стандартних підходах до УРІБ і являє собою основу ISO/IEC 27005 і BS 7799-3. Це не математична модель, але вона дає перелік і послідовність таких необхідних для управління ризиками ІБ процесів, як планування, реалізація, перевірка, дія.

На етапі планування визначаються політика та методологія управління ризиками, а також здійснюється оцінювання ризиків, яке передбачає інвентаризацію активів, складання профілів загроз і вразливостей, оцінювання ефективності контрзаходів і потенційного збитку, визначення допустимого рівня залишкових ризиків.

© Родін Є.С., 2012

На етапі реалізації виконуються роботи з обробки інформації про ризики, оцінювання критичності ризиків, планування та впровадження заходів щодо кожного з ризиків. Відповідно до результатів першого етапу керівництво організації приймає одне з чотирьох рішень стосовно кожного з ідентифікованих ризиків: проігнорувати, уникнути, передати зовнішній стороні або мінімізувати. Після цього розробляється і впроваджується план протидій по кожному з ризиків.

На етапі перевірки здійснюється аналіз функціонування відповідних механізмів мінімізації ризиків, відстежуються зміни факторів ризику (активів, загроз, вразливостей), проводяться аудити, виконуються інші процедури контролю.

На етапі дії за результатами безперервного моніторингу та проведених перевірок виконуються певні коригувальні дії, які можуть включати в себе, зокрема, переоцінювання ризиків, коригування політики і методології управління ризиками, а також план обробки ризиків [1].

2. Основний текст

Процесна модель являє собою основу для інших моделей УРІБ, направлених на стандартизацію, формалізацію й автоматизацію процесів першого та другого етапів, а саме: ідентифікація та прийняття рішення щодо обробки ризиків.

Класичні реалізації таких методик, як CRAMM, FRAP, OCTAVE, RiskWatch, базуються на використанні процесної моделі з опитувальною схемою, пропонуючи вже готові стандарти, з яких необхідно вибрати ті, що притаманні системі користувача, та оцінити їх за запропонованою системою критеріїв оцінювання:

− класифікація та певний перелік ресурсів:

◦ визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання ресурсів;

− класифікація та певний набір вразливостей:

◦ визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання вразливостей;

− класифікація та певний набір ризиків:

◦ визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання ризиків;

− класифікація та певний набір засобів і заходів безпеки:

◦ визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання вартості та надійності засобів і заходів безпеки.

Після відповідей на запитання за запропонованою схемою класичні методології УРІБ обчислюють показники та виводять за пріоритетністю перелік вразливостей, ризиків, набір протидій та дані щодо ефективності їх впровадження.

Головними цікавими відмінностями класичних методологій УРІБ є саме набір критеріїв оцінювання ресурсів, вразливостей, ризиків та формалізація обчислення кількісних показників. Наприклад, за методологією CRAMM цінність даних і програмного забезпечення визначається в таких ситуаціях:

• недоступність ресурсу протягом певного періоду часу;

• руйнування ресурсу − втрата інформації, отриманої з часу останнього резервного копіювання, або повне руйнування бази даних;

• порушення конфіденційності у випадках отримання несанкціонованого доступу штатними співробітниками або сторонніми особами;

• модифікація, яка розглядається для випадків дрібних ненавмисних помилок персоналу (помилки введення), програмних помилок, навмисних помилок;

• помилки, пов'язані з передачею інформації: відмова від доставки, неповна доставка інформації, доставка за невірною адресою.

Для оцінювання можливого збитку CRAMM рекомендує використовувати такі параметри:

• збитки для репутації організації;
• порушення чинного законодавства;
• збитки для здоров'я персоналу;
• збитки, пов'язані з розголошуванням персональних даних окремих осіб;
• фінансові втрати від розголошування інформації;
• фінансові втрати, пов'язані з відновленням ресурсів;
• втрати, пов'язані з неможливістю виконання певних зобов'язань;
• дезорганізація діяльності [2].

Програмне забезпечення CRAMM для кожної групи ресурсів і кожного із закладених у цій методології 36 типів загроз генерує список питань, що допускають однозначну відповідь. Рівень загроз оцінюється, залежно від відповідей, як дуже високий, високий, середній, низький і дуже низький, рівень вразливості − як високий, середній і низький. На основі цієї інформації розраховуються рівні ризику в дискретній шкалі з градаціями від 1 до 7.

Методика Facilitated Risk Analysis Process (FRAP) передбачає, що на початковому етапі в системі відсутні засоби і механізми захисту. Таким чином, оцінюється рівень ризику для незахищеної інформаційної системи, що надалі дозволяє показати ефект від впровадження системи захисту інформації (СЗІ).

Оцінювання здійснюється для ймовірності виникнення загрози і збитку від неї за такими шкалами.

Ймовірність (Probability):

• висока (High Probability) − дуже ймовірно, що загроза реалізується упродовж наступного року;
• середня (Medium Probability) − можливо, загроза реалізується упродовж наступного року;
• низька (Low Probability) − малоймовірно, що загроза реалізується упродовж наступного року.

Збиток (Impact) − міра величини втрат або шкоди, що наноситься активу:

• високий (High Impact) − зупинка критично важливих бізнес-підрозділів, яка призводить до істотних збитків для бізнесу, втрати іміджу або неотримання істотного прибутку;
• середній (Medium Impact) − короткочасне переривання роботи критичних процесів або систем, яке призводить до обмежених фінансових втрат в одному бізнес-підрозділі;
• низький (Low Impact) − перерва в роботі, що не спричиняє відчутних фінансових втрат.

ЙМОВІРНІСТЬ

ЗБИТОК

	Високий	Середній	Низький
Висока	A	B	C
Середня	B	B	C
Низька	B	C	D

A – роботи з виправлення мають бути виконані негайно.
B – роботи з виправлення слід виконати найближчим часом.
C – необхідно моніторити ситуацію.
D – дії з виправлення на даний не потрібні.

Рис. 1. Матриця ризику за методом FRAP

Оцінка визначається відповідно до правила, що задається матрицею ризику (рис. 1) [3].

Методика OCTAVE передбачає три фази аналізу ризику:

1) розробка профілю загроз, пов'язаних з активом;
2) ідентифікація інфраструктурних вразливостей;

3) розробка стратегії та планів безпеки.

Профіль загрози визначає актив (asset), тип доступу до активу (access), джерело загрози або суб'єкт загрози (actor), тип порушення або мотив (motive), результат (outcome) і посилання на опис загрози в загальнодоступних каталогах. Відповідно до типу джерела, загрози в OCTAVE поділяються на такі класи:

− загрози від людини-порушника, яка діє через мережу передавання даних;
− загрози від людини-порушника, яка використовує фізичний доступ;
− загрози, пов'язані зі збоями в роботі системи;
− інші.

Результатом реалізації загрози може бути розкриття (disclosure), зміна (modification), втрата або руйнування (loss/destruction) інформаційного ресурсу, відсутність доступу до ресурсу або відмова в обслуговуванні (interruption).

Методика OCTAVE пропонує скласти «профіль загроз» та «дерево варіантів». При створенні профілю загроз рекомендується уникати великої кількості технічних деталей − це завдання другої фази дослідження. А на першій потрібно стандартизованим чином описати поєднання загрози та ресурсу (активу). Наприклад, на підприємстві є інформаційний ресурс (актив) − база даних (БД) відділу кадрів (HR Database). Профіль, що відповідає загрозі класу, пов'язаного з крадіжками інформації співробітником підприємства, наведено в табл. 1, а дерево варіантів − на рис. 2 [4].

Таблиця 1. Приклад профілю загрози

Ресурс (Asset)	БД відділу кадрів (HR Database)
Тип доступу (Access)	Через мережу передачі даних (Network)
Джерело загрози (Actor)	Внутрішня (Inside)
Тип порушення (Motive)	Навмисне (Deliberate)
Вразливість (Vulnerability)	Помилка при делегуванні прав доступу Неблагонадійність співробітників
Наслідки (Outcome)	Розкриття даних (Disclosure)
Посилання на каталог вразливостей (Catalog reference)	US-CERT

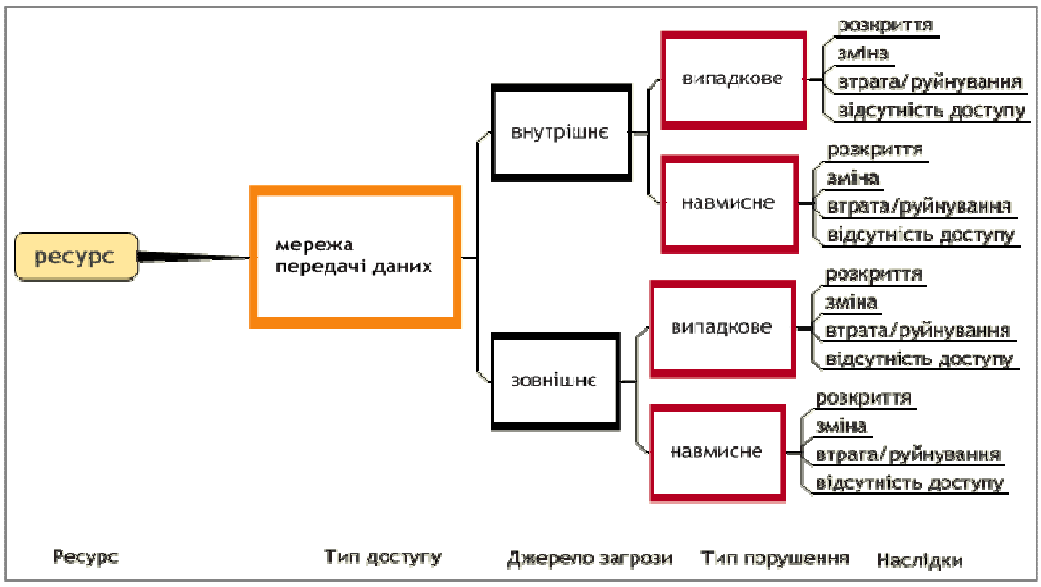

Рис. 2. Дерево варіантів, що використовується при описі профілю загрози

Група дослідників, що проводить аналіз для кожного сегмента мережі, визначає, які компоненти в ньому перевіряються на наявність вразливостей. Вразливості виявляються сканерами безпеки рівня операційної системи, мережевими сканерами безпеки, спеціалізованими сканерами (для конкретних web-серверів, СКБД тощо) за допомогою списків вразливостей (checklists), тестових скриптів.

Для кожного компонента визначаються:

• список вразливостей, які потрібно усунути негайно (high-severity vulnerabilities);

• список вразливостей, які потрібно усунути найближчим часом (middle-severity vulnerabilities);

• список вразливостей, які не вимагають негайних дій (low-severity vulnerabilities).

За результатами цієї фази формується звіт із зазначенням списку виявлених вразливостей, впливу, який вони можуть здійснити на виділені раніше ресурси (активи), а також заходів щодо усунення вразливостей.

Розробка стратегії та планів безпеки − третя фаза дослідження системи. Вона починається з оцінювання ризику, яке проводиться на базі звітів за двома попередніми фазами. В OCTAVE дається лише оцінка очікуваного збитку, без визначення ймовірності реалізації загрози. Шкала оцінювання ризику: високий (high), середній (middle), низький (low). Обчислюються фінансові збитки, збитки стосовно репутації компанії, життя та здоров'я клієнтів і співробітників, збитки, що їх може викликати судове переслідування в результаті того або іншого інциденту. Описуються значення, відповідні кожній градації шкали (наприклад, для малого підприємства фінансові збитки в $10000 є високими, для великого − середніми).

Розглянуті вище моделі УРІБ базуються на процесній моделі і пропонують якісні й кількісні показники оцінювання ризиків. У більшості випадків, якщо показник має якісну характеристику, то цю якість прив’язують до чисельної шкали й перетворюють показник у кількісний. Розглянемо декілька підходів до формалізації обчислення ризиків.

Класична формула − оцінювання ризику виконується за двома факторами: ймовірність реалізації загрози (Рреалізації) і розмір збитку (Збиток):

$$Ризик = P_{реалізації} \times Збиток .$$

Подальша деталізація ймовірності реалізації загрози може бути визначена формулою, яка враховує ймовірність виникнення загрози та ймовірність появи вразливості:

$$P_{реалізації} = P_{загрози} \times P_{вразливості} .$$

У методиці RiskWatch формула обчислення ризику зазнала певних змін у зв'язку з тим, що RiskWatch використовує визначені Американським інститутом стандартів (NIST) оцінки, які називаються LAFE і SAFE. LAFE (Local Annual Frequency Estimate), і показує, скільки разів на рік в середньому певна загроза буде реалізована в даному місці (наприклад, в межах цього міста). SAFE (Standard Annual Frequency Estimate) визначає, скільки разів на рік в середньому певна загроза буде реалізована в цій "частині світу" (наприклад, в Північній Америці). Вводиться також поправковий коефіцієнт, який дозволяє врахувати, що в результаті реалізації загрози захищуваний ресурс може бути знищений не повністю, а лише частково. Отже, оцінка ризику за методикою RiskWatch розраховується як оцінка очікуваних річних втрат:

$$ALE = AssetValue \times ExposureFactor \times Frecuency ,$$

де Asset Value − вартість даного активу (даних, програм, апаратури і т.д.);

Exposure Factor − коефіцієнт дії, що показує, яка частина (у відсотках) від вартості активу піддається ризику;

Frequency − частота виникнення небажаної події;

ALE − оцінка очікуваних річних втрат для одного конкретного активу від реалізації однієї загрози [7].

Більшість інших методів обчислення рівня ризиків являють собою різні модифікації наведених вище формул. Наприклад, рівень ризику по всій системі – це сума ризиків по всіх активах та кожній загрозі; ефект від вжитих контрзаходів обчислюється як різниця між сумою запланованих витрат на контрзаходи та сумарною оцінкою збитків при визначеному рівні ризику по всій системі.

3. Заключення

Базою для визначення рівня ризику, як бачимо з розглянутих формул, майже в усіх методиках є ймовірність виникнення тієї чи іншої події, яка впливає на ймовірність реалізації загрози. У більшості методик визначення ймовірності здійснюється експертним методом або за базу береться статистика минулих періодів щодо таких самих подій.

Чи відповідає така методика реаліям, наскільки вона точна? По-перше, необхідно внести поправку на помилку експертів, по-друге, статистика минулих періодів не буде відповідати реальності, особливо у випадках швидкої зміни програмного та технічного забезпечення (вразливості якого ще невідомі).

Отже, якщо дослідник вирішив своїми силами точніше визначити рівень ризику інформаційної безпеки, то йому потрібна додаткова інформація, для отримання якої слід організувати:

1. Ретельний аналіз, інжиніринг системи на предмет кристалізації (з певною мірою абстракції) всіх подій, наслідком яких може бути втрата, пошкодження ресурсу (наприклад, порушення конфіденційності, доступності, цілісності інформації). Тобто необхідно побудувати дерево (або дерева) всіх подій і станів у системі, які можуть призвести до втрат. Іншими словами, для однієї загрози можуть бути декілька вразливостей і навпаки або одна вразливість не завжди веде до виникнення загрози, але може призвести до появи ще двох вразливостей, що спричинять реалізацію загрози.

Такий аналіз базується на дослідженні роботи всієї системи й передбачає вивчення:

− архітектури системи;
− інформаційних потоків системи з можливими станами;
− роботи всіх суб’єктів системи (всі можливі дії);
− роботи програмного забезпечення (всі можливі стани);
− роботи технічних засобів (усі можливі стани).

2. Визначення для кожної події (з побудованого дерева подій) ймовірності реалізації найгіршого сценарію. Якщо спробувати знайти альтернативу експертним оцінкам, то можна звернутися до побудови імітаційних моделей подій, процесів, поведінки, наприклад:

− модель роботи технічних засобів;
− модель роботи програмного забезпечення;
− модель атаки DoS;
− модель поведінки порушника;
− модель роботи СЗІ;
− модель роботи користувача.

Таким чином, у кожному конкретному випадку розробки моделі управління ризиками інформаційної безпеки необхідно вибрати таку модель або комбінацію моделей, яка брала б до уваги якомога більше результуючих факторів, притаманних даній системі, та найбільш достовірно визначала ймовірність реалізації найгіршого сценарію для кожної події з дерева подій, сформованого за результатами інжинірингу системи (п. 1). При цьому така модель повинна динамічно змінювати вихідні результати при зміненні масштабу та якості суб’єктів і об’єктів системи, наприклад: кількість користувачів, кількість комутаційного обладнання, швидкість каналу передавання даних. Також модель має враховувати

можливі зміни в дереві процесів і станів (такі зміни, безумовно, будуть мати місце, наприклад, у разі вдосконалення СЗІ).

СПИСОК ЛІТЕРАТУРИ

1. International standard BS ISO/IEC 27005:2008, 2008-06-15.
2. A Qualitative Risk Analysis and Management Tool – CRAMM. – Bethesda, Maryland: SANS Institute, 2002. – 15 p.
3. Visintine V. An Introduction to Information Risk Assessment / Visintine V. – Bethesda, Maryland: SANS Institute, 2003. – 13 p.
4. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process / Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson. − Carnegie Mellon University, 2007. – 154 p.
5. Информационная безопасность [Электронный ресурс]. – Режим доступа: http://inf-bez.ru.
6. Кириличев Б.В. Моделирование систем / Б.В. Кириличев. – М.: МГИУ, 2009. – 274 с.
148. James J. Cebula A Taxonomy of Operational Cyber Security Risks / James J. Cebula, Lisa R. Young. – Hanscom AFB, MA: Carnegie Mellon University. – 47 p.
8. Gary Stoneburner. Risk Management Guide for Information Technology Systems / Stoneburner G., Goguen1 A., Feringa1 A. – Gaithersburg: National Institute of Standards and Technology, 2002. – 55 p.
9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. – ФСТЭК России, 2008. – Режим доступа: http://securitypolicy.ru.

Стаття надійшла до редакції 21.08.2012