УДК 621.392

О.Г. Пузиренко[1], С.О. Івко[2], О.О. Лаврут[2], О.К. Климович[2]

[1] *Генеральний штаб Збройних Сил України, Київ*
[2] *Академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів*

ЗАСТОСУВАННЯ МОДЕЛЕЙ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Проведено аналіз процесу роботи найбільш поширених моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. Розкрито основні підходи до оцінювання ризиків інформаційної безпеки. Вказано на недосконалості зазначених методологій і запропоновано шляхи побудови більш функціональних моделей управління ризиками інформаційної безпеки.

***Ключові слова**: захист інформації, інформаційно-телекомунікаційні системи, ризики інформаційної безпеки.*

Вступ

Постановка проблеми в загальному вигляді. Пріоритетними напрямками наукових досліджень в області інформаційної безпеки вважається: розробка моделей загроз безпеки ІТС і способів їх реалізації, визначення критеріїв вразливості й стійкості систем до деструктивних впливів, розробка методів і засобів моніторингу для виявлення фактів застосування несанкціонованих інформаційних впливів, розробка методології й методичного апарата оцінки збитку від впливу погроз інформаційної безпеки.

Не менш нагальною задачею для забезпечення інформаційної безпеки виступає розробка методів і засобів забезпечення інформаційної безпеки інформаційних і телекомунікаційних систем, у тому числі автоматизованих систем керування безпекою, методів і засобів розподілу ключів і захисту інформації й інформаційних ресурсів від несанкціонованого доступу й руйнуючого інформаційного впливу, антивірусних технологій, методів і засобів контролю стану захищеності від несанкціонованого доступу сучасних і перспективних технічних засобів і каналів зв'язку, розв'язок проблеми гарантованого знищення залишкової інформації на магнітних носіях, дослідження й розвиток методів побудови захищених систем, що використовують ненадійні (з погляду інформаційної безпеки) елементи, включаючи проблему їх тестування

Нагальні здачі випливають з стрімкого розвитку інформаційно-телекомунікаційних систем що на сьогодні перетворюються на розподілені системи з безліччю об’єктів, суб’єктів, з різноманітними інформаційними потоками і зв’язками. 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.

Аналіз останніх досліджень і публікацій. Ключовою моделлю, що використовується 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.

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 ризи-

ків, 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].

Тому **метою** даної роботи є передумови для створення процесної моделі, яка 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 інформаційної безпеки.

Основна частина

Огляд класичних методик управління ризиками інформаційної безпеки

Класичні реалізації таких методик, як CRAMM, FRAP, OCTAVE, Risk Watch, 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 [2]:

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 [3].

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 [4]:

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.

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 рези-ку 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 (Р):

висока − дуже ймовірно, що загроза реалізується упродовж наступного року;

середня − можливо, загроза реалізується упродовж наступного року;

низька − малоймовірно, що загроза реалізується упродовж наступного року.

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

високий − зупинка критично важливих бізнес підрозділів, яка призводить до істотних збитків для

бізнесу, втрати іміджу або отримання істотного прибутку:

середній − короткочасне переривання роботи критичних процесів або систем, яке призводить до обмежених фінансових втрат в одному бізнес-підрозділі;

низький − перерва в роботі, що не спричиняє відчутних фінансових втрат.

Оцінка визначається відповідно до правила [5], що задається матрицею ризику (табл. 1), де A – роботи з виправлення мають бути виправленні негайно; B – роботи з виправленням слід виконувати найближчим часом; C – необхідно моніторити ситуацію; D – дії з виправлення на даний час не потрібні.

Таблиця 1

Матриця ризику за методом FRAP

P \ I	Високий	Середній	Низький
Висока	A	B	C
Середня	B	B	C
Низька	B	C	D

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 ресурс, тип доступу до ресурсу, джерело загрози або суб'єкт загрози, тип порушення, результат 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;

Результатом реалізації загрози може бути розкриття, зміна, втрата або руйнування інформаційного ресурсу, відсутність доступу до ресурсу або відмова в обслуговуванні.

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. Наприклад, на підприємстві є інформаційний ресурс − база даних (БД) відділу кадрів. Профіль, що відповідає загрозі класу, пов'язаного з крадіжками інформації співробітником підприємства, наведено в табл. 2, а дерево варіантів − на рис. 1 [6].

Таблиця 2

Профіль загрози за методом OCTAVE

Ресурс	БД відділу кадрів
Тип доступу	Через мережу передачі даних
Джерело загрози	Внутрішня
Тип порушення	Навмисне
Вразливість	Помилка при делегуванні прав доступу Неблагонадійність співробітників
Наслідки	Розкриття даних
Посилання на каталог вразливостей	US-CERT

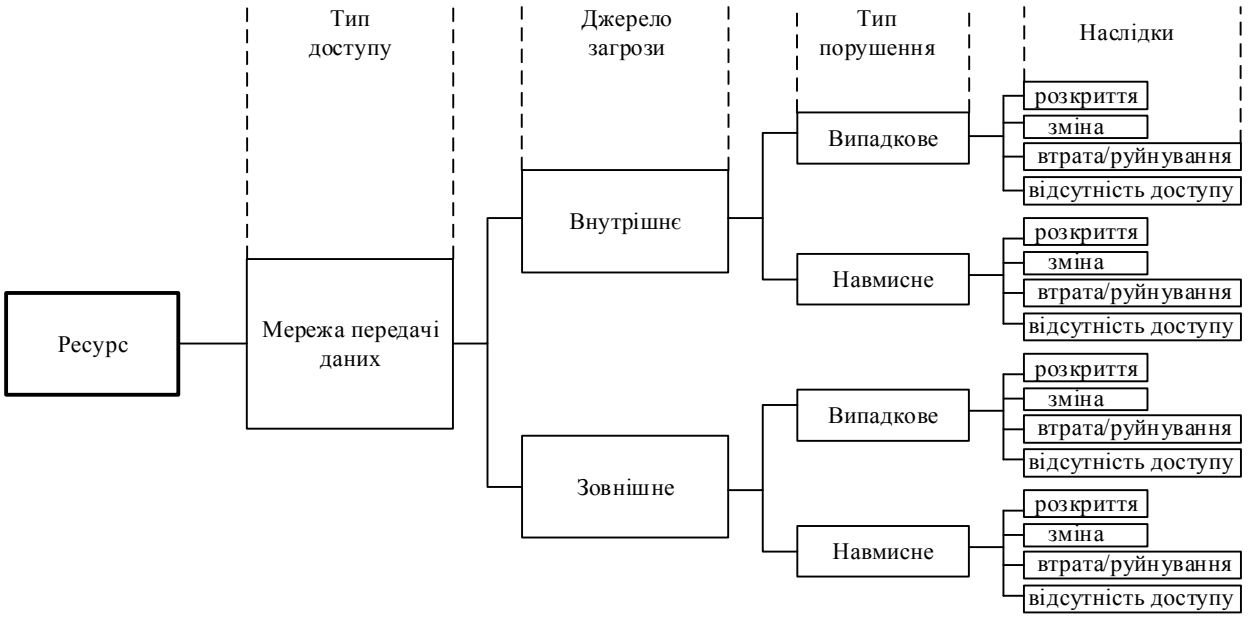

Рис. 1. Дерево варіантів, що використовується при описі профілю загрози

Група експертів, 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, систем керування БД тощо) за допомогою списків вразливостей, тестових скриптів.

Для кожного компонента визначаються:

– список вразливостей, які потрібно усунути негайно;

– список вразливостей, які потрібно усунути найближчим часом;

– список вразливостей, які не вимагають негайних дій.

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 [7].

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, середній, низький. 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.

Як приклад в [8] запропонована адаптована методика управління ризиками при забезпеченні живучості та неперервності функціонування СЗІ в інформаційно-телекомунікаційних системах на основі методики OCTAVE. Адаптована методика управління ризиками при забезпеченні живучості та неперервності функціонування СЗІ в ІТС враховує позитивні якості основних методик і мінімізує їх недоліки.

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. Local Annual Frequency Estimate (LAFE) показує, скільки разів на рік в середньому певна загроза буде реалізована в даному місці (наприклад, в межах міста). Standard Annual Frequency Estimate (SAFE) визначає, скільки разів на рік в середньому певна загроза буде реалізована в цій "частині світу" (наприклад, в Північній Америці). Вводиться також поправочний коефіцієнт, який дозволяє врахувати, що в результаті реалізації загрози ресурс, що необхідно захистити може бути знищений не повністю, а лише частково [9].

Отже, оцінка ризику за методикою RiskWatch розраховується як оцінка очікуваних річних втрат для одного конкретного ресурсу від реалізації однієї загрози ALE:

$$ALE = AV \times EF \times F,$$

де AV − вартість даного активу (даних, програм, апаратури); EF − коефіцієнт дії, що показує, яка частина (у відсотках) від вартості активу піддається ризику; F − частота виникнення небажаної події;

Основні підходи до оцінювання ризиків інформаційної безпеки

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 [10] − оцінювання ризику (R) виконується за двома факторами: ймовірність реалізації загрози ($P_{реалізації}$) і розмір збитку (D):

$$R = P_{реалізації} \times D.$$

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

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

Більшість інших методів обчислення рівня ризиків інформаційної безпеки 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.

Висновки

Виходячи з вищезазначеного, базою для визначення рівня ризику 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.

Але наведений підхід не буде в повній мірі відповідати реальному рівню ризику інформаційної безпеки. 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, для більш точного визначення рівеня ризику інформаційної безпеки, потрібна додаткова інформація, для отримання якої слід провести:

– 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).

– визначення для кожної події (з побудованого дерева подій) ймовірності реалізації найгіршого сценарію. Якщо спробувати знайти альтернативу експертним оцінкам, то є можливість 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. 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) [11].

Список літератури

1. Information technology – Security techniques – Information security risk management: ISO/IEC 27005:2008. – [Чинний від 15-06-2008]. — Женева: [б.в.], 2008. – 64 с. – (Міжнародні стандарти ISO/IEC).

2. Иванов С.П. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных / С.П. Иванов. – М.: Научная мысль, 2008. – 108 с.

3. Хорошко В.О. Методичний підхід щодо оцінки рівня безпеки інформації / В.О. Хорошко, В.С. Чередниченко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Вип. № 14 – К.: ВІКНУ, 2008. – С. 176-181.

4. Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; – К.: ДУІКТ, 2008. – 186 с.

5. Балашов П.А. Оценка рисков информационной безопасности на основе нечёткой логики / П.А. Балашов, Р.И. Кислов, В.П. Безгузиков // Безопасность компьютерных систем. Конфидент. – 2003. – № 6. – С. 60-65.

6. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев; – К.: ООО "ТИД", 2004. – 912 с.

7. Кириличев Б.В. Моделирование систем / Б.В. Кириличев. – М.: МГИУ, 2009. – 274 с.

8. Пузиренко О.Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем / О.Г. Пузиренко, С.О. Івко, О.О. Лаврут // Системи обробки інформації .- Х.: ХУПС,; 2014. – Вип. 8 (124). – С. 128-134.

9. Чередниченко В.С. Обґрунтування пріоритетних заходів, щодо підвищення рівня інформаційної безпеки / В.С. Чередниченко // Захист інформації, – 2008. – № 4. – С.13-15.

10. Козелецкий Ю.А. Психологическая теорія решений / Ю.А. Козелецкий; – М.: Прогресс, 1979. – 504 с.

11. Родін Є.С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки / Є.С. Родін // Математичні машини і системи. – 2012. – № 4. – С. 178-180.

Надійшла до редколегії 15.01.2015

Рецензент: д-р техн. наук, ст. наук. співр. М.А. Яковлев, Академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів.

ПРИМЕНЕНИЕ МОДЕЛЕЙ ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

О.Г. Пузыренко, С.А. Ивко, А.А. Лаврут, О.К. Климович

Проведен анализ процесса работы наиболее распространенных моделей оценивания рисков информационной безопасности в информационно-телекоммуникационных системах. Раскрыты основные подходы к оцениванию рисков информационной безопасности. Указано на несовершенство указанных методологий и предложены пути построения более функциональных моделей управления рисками информационной безопасности.

Ключевые слова: *защита информации, информационно-телекоммуникационные системы, риски информационной безопасности.*

APPLICATION OF THE INFORMATION SECURITY RISK ASSESSMENT MODEL IN INFORMATION AND TELECOMMUNICATION SYSTEMS

O.G. Puzyrenko, S.O. Ivko, O.O. Lavrut, O.K. Klimovich

The most common information security risk assessment model in information and telecommunication systems work was analyzed. The main approaches to the information security risks evaluation were outlined. The imperfections of these methodologies and ways to build a more functional information security risk management were given.

Keywords: *information security, information and telecommunication systems, information security risks.*