УДК 004.056.5
DOI: 10.18372/2310-5461.35.11841

С. С. Бучик, д-р техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова
orcid.org/0000-0003-0892-3494

e-mail: s_stbu@ukr.net;

В. О. Шалаєв
Житомирський військовий інститут імені С. П. Корольова
orcid.org/0000-0002-2633-9219
e-mail: 301vadim.s@ukr.net

АНАЛІЗ ІНСТРУМЕНТАЛЬНИХ МЕТОДІВ ВИЗНАЧЕННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Актуальність дослідження

Рівень інформаційного суспільства провідної держави світу характеризується показниками сучасних наукоємних технологій у яких відіграють основну роль інформаційно-телекомунікаційні системи (ІТС).

Захист інформації є важливою складовою частиною підтримання національної безпеки України. Організація захисту інформації здійснюється за допомогою системи правових, організаційних та інженерно-технічних заходів. Розвиток національної безпеки і оборони держави залежить від взаємодії та спільного використання інформаційних технологій об'єднаних у єдиний інформаційно-телекомунікаційний простір.

Сучасний етап розвитку нашої держави визначається соціально-політичною та економічною нестабільністю різних суспільних факторів, які приводять до ведення інформаційних війн. У протидії інформаційним війнам слід приділяти велику увагу захисту державним інформаційним ресурсам. Адже загрози інформаційної безпеки держави відіграють головну роль в системі захисту ІТС [1, с. 16].

Визначення терміну «інформаційна безпека» (ІБ) у більш вузькому значенні має характер процесу забезпечення конфіденційності, цілісності та доступності. Існує досить великий клас систем обробки інформації, під час розробці яких фактор безпеки відіграє першорядну роль (наприклад, банківські, інформаційні, медичні, економічні та лінгвістичні системи).

Одним з важливих організаційних заходів захисту інформації в комп'ютеризованих системах є визначення переліку загроз інформації, які порушують її властивості – конфіденційність, цілісність та доступність. Одна або декілька загроз можуть використовувати ряд уразливостей інформації.

Будь-яка зміна загроз та уразливостей може мати значний вплив на ІБ. Раннє виявлення або знання про ці зміни збільшує можливості щодо прийняття необхідних заходів для обробки ризику та забезпечення безпеки ІТС у цілому. Це досягається за рахунок інструментальних методів визначення ризиків інформаційної безпеки в ІТС.

Таким чином ***метою*** статті є проведення аналізу існуючих інструментальних методів визначення ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах, що і зумовлює актуальність тематики статті.

Аналіз останніх досліджень і публікацій

Питання аналізу ризиків інформаційної безпеки висвітлені у наукових працях та інформаційно-довідкових матеріалах. Проблемами дослідження інформаційної безпеки в ІТС займаються як вітчизняні вчені (Горбенко І. Д., Домарєв В. В., Корченко О. Г., Юдін О. К.), так і зарубіжні (Астахов А. М., Daniel Wentre, Thomas R., Whitman M.).

У праці [1, с. 2] проведено аналіз сучасного забезпечення захисту державних інформаційних ресурсів (ДІР) в ІТС. Проведено аналіз та систематизовано підходи до класифікації загроз інформаційним ресурсам у цілому. В монографії проведено нормативно-правовий аналіз напрямів, пов'язаних із впровадженням реєстру державних

електронних інформаційних ресурсів, досліджено шляхи подальшої реалізації проблематики, в тому числі шляхом подальшого розроблення інструментального засобу аналізу ризиків ІБ ДІР.

У праці [2, с. 138] розглянуто підходи і програмні рішення оцінки і контролю інформаційних ризиків як фундаментального організаційного етапу при побудові системи захисту інформації комп'ютеризованих систем.

У праці [3, с. 128] проведено аналіз процесу управління ризиками інформаційної безпеки в контексті забезпечення неперервності функціонування система захисту інформації. Надана оцінка процесу управління ризиками, проаналізовані сучасні методики управління ризиками інформаційної безпеки. Запропоновано удосконалений алгоритм адаптованої методики управління ризиками при забезпеченні живучості та неперервності функціонування системи захисту інформації в інформаційно-телекомунікаційній системи.

У праці [4, с. 33] запропоновано та проаналізовано удосконалену методику оцінювання інформаційного ризику в автоматизованій системі. Висвітлено необхідні нормативно-правові документи інформаційної безпеки. Розглянуто роботу прототипу експертної системи, яка дозволяє оцінити рівень інформаційного ризику для певної автоматизованої системи та визначити необхідність застосування додаткових заходів інформаційної безпеки.

У праці [5, с. 75] проведено аналіз процесу роботи найбільш поширених моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. Розкрито основні підходи до оцінювання ризиків інформаційної безпеки.

У праці [6, с. 60] розглянуто програмні продукти аналізу та управлінням інформаційними ризиками. Одержано чітку структуру функціонування програм: розкрито алгоритмічні принципи побудови, формати шаблонів, графічні інтерфейси, методики управління та визначення рівня загрози ризику. Проаналізовано програмні продукти управлінням інформаційними ризиками на відповідність вимогам основних міжнародних стандартів інформаційної безпеки.

У праці [7, с. 2] розглянуто підходи і програмні рішення оцінки і контролю інформаційних ризиків як фундаментального організаційного етапу при побудові системи захисту інформації комп'ютеризованих систем.

Постановка завдання

Виходячи з поставленої мети, необхідно здійснити аналіз існуючих інструментальних методів оцінювання та управління ризиками в інформаційно-телекомунікаційних системах з використанням вимог сучасних стандартів у галузі управління інформаційною безпекою та провести аналіз їх основних характеристик.

Виклад основного матеріалу

З розвитком інформаційних технологій на сьогодні постає проблема забезпечення інформаційної безпеки та технічного захисту інформаційних ресурсів в комп'ютеризованих системах [2, с. 138].

Як показує огляд інформаційних джерел, у галузі оцінки та управління інформаційними ризиками в ІТС на даний момент переважають інструментальні засоби їх оцінки такі, як CRAMM, Risk Watch, ГРИФ 2006, NIST, COBRA, OCTAVE. Оцінка ризиків є зараз одним з актуальних напрямків у сфері регулювання банківської діяльності.

У загальному випадку можна виділити такі складові управління ризиками [4, с. 36–37]:

1. Моніторинг та оцінювання організаційних ризиків функціонування системи.

2. Моніторинг та оцінювання ризиків технічних засобів.

3. Прийняття рішення з управління ризиками на основі наявних оцінок.

4. Проведення безпосередньої роботи з управління ризиками.

Умовно проблематику аналізу ризиків можна поділити на дві групи. До першої належить розроблення наукових методів аналізу ризиків на основі відомих теорій та вимог стандартів щодо створення системи управління інформаційної безпеки (СУІБ). Друга група містить спеціалізовані програмні продукти, які, зазвичай базуються на методах першої групи, але мають більшу практичну спрямованість і краще враховують специфіку об'єкта захисту.

Серед існуючих загроз, що сформувалися з розвитком інформаційних технологій, важливу роль необхідно приділити засобам впливу на інформаційну інфраструктуру ІТС та захищеність ДІР (комп'ютерні віруси, мережеві «трояни», які спотворюють, знищують інформацію та здійснюють інші види комп'ютерної злочинності).

Відповідно до стандартів ISO/IEC 27005 та ISO/IEC TR 13335-2 оцінювання ризиків включає такі етапи:

1. Оцінку ймовірності можливих загроз і уразливостей.

2. Розрахунок ступеню впливу, який може мати загрозу на кожен актив.

3. Визначення кількісної (виміряної) або якісної (описуваної) вартості ризику.

Оцінювання ризиків полягає у визначенні кількісних та якісних показників, формуванні реєстру ризиків та ранжируванні ризиків [11].

Метод, який використовується для роботи вибраного продукту оцінювання ризиків ІБ ІТС повинен з високою ефективністю відображати формування звітів про результати оцінки ризиків. Ефективність використання продукту залежить від того, на скільки добре користувач його розуміє, а також від правильності встановлення та налаштування даного продукту [11].

З аналізу інструментальних методів визначення ризиків інформаційної безпеки, які є найбільш поширеними для вирішення задачі протиборства інформаційним загрозам в ІТС, схема інструментальних методів визначення ризиків інформаційної безпеки може бути приведена до вигляду рис. 1.

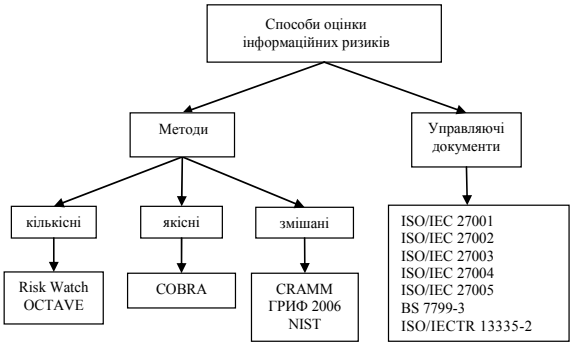

Рис. 1. Схема інструментальних методів визначення ризиків інформаційної безпеки в ІТС

Автор праці [12, с. 424] вважає, що при розробці методу визначення оцінки ризиків ІБ обов'язково повинне проводитися оцінювання граничнодопустимого та існуючого ризику виникнення загрози протягом деякого часу. А для цього має бути отримані значення вірогідності виникнення загрози на протязі певного часу. Практика показує, що для більшості існуючих загроз неможливо отримати достовірні дані про вірогідність реалізації загрози, тому для вирішення цієї проблеми існують методи кількісної оцінки визначення ризиків ІБ. При розробці методу визначення ризиків можуть бути використані методи системного аналізу. Проаналізуємо методи визначення ризиків ІБ, які найбільш поширені в ІТС та банківських структурах для забезпечення захисту інформації та визначення ризиків, які переростають в потенційну загрозу.

Британський CRAMM (the UK Government Risk Analysis and Management Method). Інтерфейс інструментального засобу оцінювання ризиків ІБ CRAMM наведено на рис. 2.

Метод CRAMM був розроблений службою безпеки Великої Британії та взятий на озброєння як державний стандарт. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, який поєднує кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій для отримання відповідних результатів економічного обґрунтування витрат організації на забезпечення інформаційної безпеки [9, с. 80].

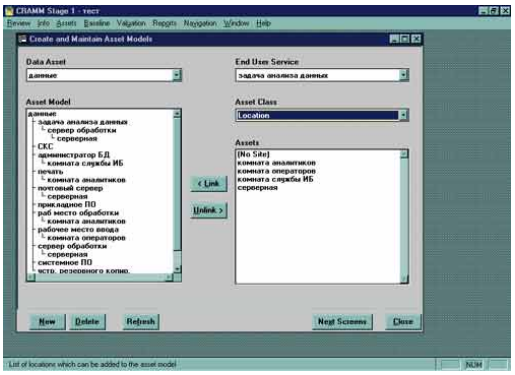

Рис. 2. Інтерфейс методу CRAMM

Метод CRAMM має базу знань по ризикам і видам їх мінімізації, засоби збору інформації, формування звітів, а також реалізує алгоритм для визначення величини ризику [11].

Метод CRAMM пропонує всі процедури методу поділити на три послідовних етапи, які розглянуто на рис. 3.

У метод CRAMM закладено широкий набір типових рекомендацій щодо проведення контрзаходів для зменшення ризиків ІБ ІТС, але її ефективне використання можливе тільки фахівцями вищої кваліфікації.

Перевагами методу CRAMM:

– даний метод є універсальним і підходить, як для державного, так і комерційного використання;

– має властивість кількісної та якісної оцінки ризиків;

– оптимальні затрати на засоби контролю та захисту інформації;

– оперативність в прийнятті рішення з питань управління безпекою [9, с. 89].

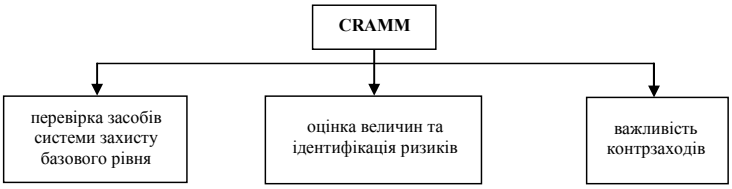

Рис. 3. Етапи проведення аналізу ризиків ІБ методом CRAMM

До недоліків CRAMM можна віднести:

– використання даного методу вимагає спеціальної підготовки користувача;

– потребує велику кількість годин безперервної роботи з аналізу інформації;

– відсутня можливість внесення додатків у базу даних та знань;

– припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як «уникнення» або «прийняття», не розглядаються;

– програмне забезпечення CRAMM існує тільки на англійській мові [3, с. 131];

– дане програмне забезпечення є платним — вартість від $ 2000 до $ 5000.

Наступним програмним забезпеченням є експертна система **Risk Watch** (розроблений компанією Risk Watch), яка презентує себе як потужний засіб аналізу та управління ризиками. Інтерфейс експертної системи аналізу та управління ризиками ІБ Risk Watch представлено на рис. 4. RiskWatch являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів [11, 5, с. 76].

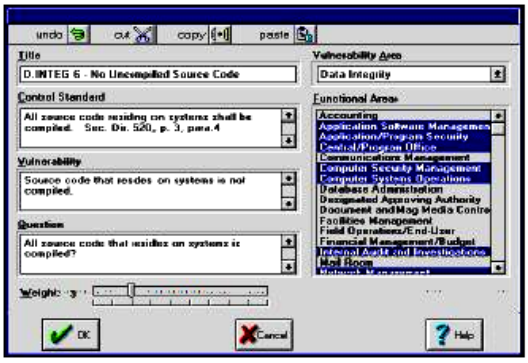

Рис. 4. Інтерфейс методу RiskWatch

Система Risk Watch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту ІБ в ІТС.

Даний метод забезпечує проведення аналізу ризиків ІБ та включає чотири етапи роботи, які представлено на рис. 5 [5, с. 76].

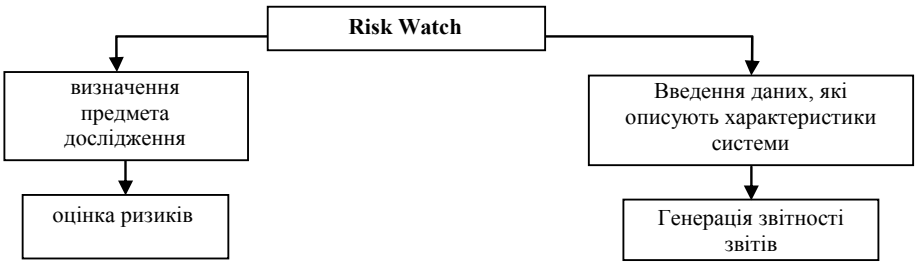

Рис. 5. Етапи проведення аналізу ризиків ІБ методом Risk Watch

У результаті аналізу експертної системи Risk Watch можна дійти висновку, що трудомісткість робіт з аналізу ризиків цим методом порівняно невелика. З точки зору вітчизняного споживача порівняльною характеристикою Risk Watch є його простота, мала трудомісткість перекладу інтерфейсу і велика гнучкість, що забезпечує можливість створення своїх нових профілів захищеності та є основною перевагою даного методу.

До недоліків Risk Watch можна віднести:

– метод ефективний лише при проведенні аналізу ризиків на програмно-технічному рівні захисту без урахування організаційних і адміністративних чинників;

– дане програмне забезпечення англомовне;

– висока вартість ліцензії — $ 15000.

На основі цього методу вітчизняні розробники можуть створювати свої профілі, що відбивають вітчизняні вимоги у сфері безпеки, розробляти відомчі методики аналізу і управління ризиками [2, с. 141].

На рис. 6 представлено інтерфейс методу ГРИФ 2006.

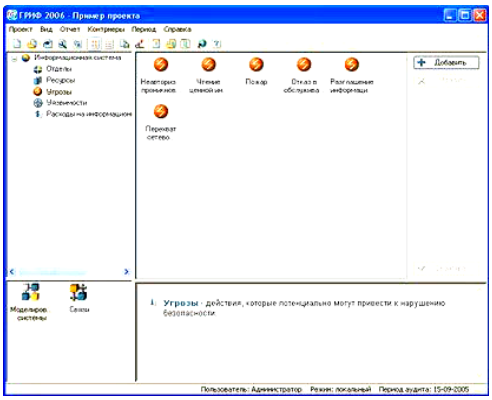

Рис. 6. Інтерфейс методу ГРИФ 2006

Для побудови повної моделі автоматизованої системи з погляду ІБ є програмний комплекс **ГРИФ 2006** з достатньо простим та зрозумілим для користувача інтерфейсом.

Основним завданням даного методу — надати можливість користувачу самостійно (без залучення сторонніх експертів) оцінити рівень ризиків в інформаційній системі, оцінити ефективність існуючої практики щодо забезпечення без-

пеки системи. Для визначення рівня ризиків в інформаційній системі метод ГРИФ 2006 передбачає такі етапи роботи, які розглянуто на рис. 7.

Метод ГРИФ 2006 має модуль управління ризиками, який надає змогу проаналізувати всі причини того значення ризику, який отримується після обробки алгоритмів занесених даних.

Отже знаючи причини інформаційного ризику користувач буде володіти всіма даними необхідними для реалізації контрмір [8, с. 55].

У результаті роботи методу ГРИФ формується звіт рівня ризику за систему, причини виникнення ризику та аналіз уразливостей з оцінкою економічної ефективності всіх можливих контрмір.

Перевагами методу ГРИФ 2006 є:

– просте в використанні програмне рішення оцінки рівня ризиків в ІТС;

– можливість здійснення оцінки ризиків по різним інформаційним ресурсам;

– ефективність управління ризиками за допомогою вибору контрзаходів;

– не потребує спеціальних знань у сфері інформаційної безпеки.

До недоліків ГРИФ 2006 можна віднести:

– відсутність прив'язки до бізнес-процесів;

– відсутня можливість зрівнювання звітності на різних етапах втілення комплексу мір із забезпечення захищеності інформації.

Метод **NIST** (National Institute of Standards and Technology) є методом оцінки ризиків Національного інституту стандартів і технологій США.

Запропонований процес управління ризиками ІБ представлено на рис. 8.

Рис. 7. Етапи методу ГРИФ 2006 для оцінки рівня ризиків в інформаційній системі

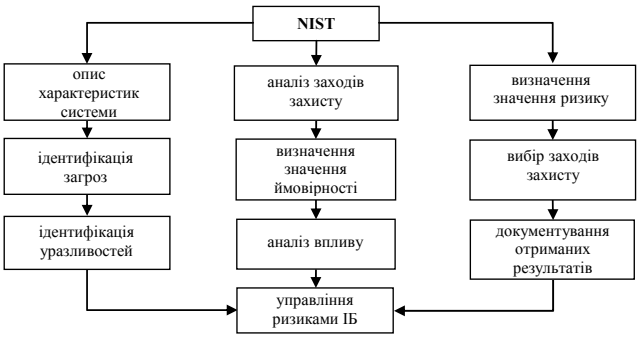

Рис. 8. Поетапний порядок роботи методу NIST

Цей метод передбачає попереднє оцінювання двох параметрів: потенційного збитку і ймовірності можливого інциденту. Такий механізм отримання оцінки ризику значно обмежує точність результатів, забезпечуючи при цьому оперативність та відтворюваність. Реалізація загрози ІБ в даному методі охоплює широке коло завдань, головним з яких є розроблення власної системи управління ризиками [3, с. 129].

Аналізуючи працю автора [2] можна дійти висновку, що дана методика охоплює широке коло завдань, які пов'язані з управлінням інформаційних ризиків і є основою для побудови власної системи управління ризиками. Інтерфейс методу NIST представлено на рис. 9.

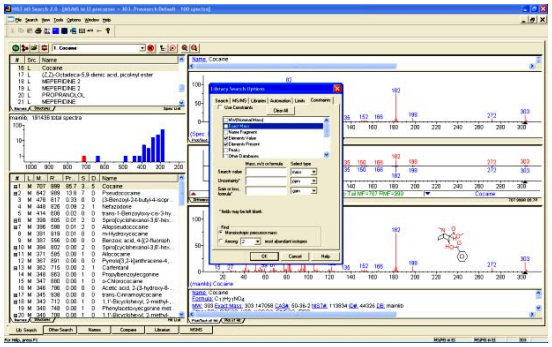

Рис. 9. Інтерфейс методу NIST

Перевагами методу NIST є:

– порівняно простий в реалізації;

– детально описує всі можливі ризики для інформаційних активів;

– припускає використання способів зниження ризиків усіх можливих варіантів (прийняття, зниження, перенесення, уникнення ризику);

– програмному забезпеченню властива відносна легкість та зручність у використанні;

– не велика вартість ліцензії порівняно з іншими подібними експертними системами $ 149–$ 254.

До недоліків NIST можна віднести:

– довготривалий процес аналізу;

– програмне забезпечення розроблено на англійській мові;

– потребує спеціальних знань в області ІБ;

– аналіз ризику проводиться за трирівневою шкалою.

Метод **COBRA** (Consultative Objective and Bi-Functional Risk Analysis, developer — C & A Systems Security Ltd, Велика Британія) орієнтований на підтримку вимог стандарту ISO 17799.

У комплект програмного забезпечення (ПЗ) входять модулі COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant, а також менеджер модуля COBRA, який призначений для налаштування та зміни наявної бази знань [10].

Цей метод дозволяє виконати в автоматизованому режимі найпростіший варіант оцінювання інформаційних ризиків будь-якого підприємства. Він оцінює відносну важливість усіх загроз і уразливостей, генерує відповідні рішення та рекомендації.

Для цього пропонується використати спеціальні електронні бази знань та процедури логічного виводу, які відповідають вимогам відповідних стандартів [8].

Аналіз ооцінювання ризиків на основі тематичних запитів проводиться за наступними категоріям, які розглянуто на рис. 10 [10].

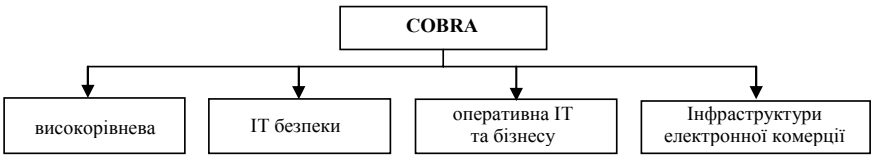

Рис. 10. Етапи оцінювання ризиків на основі тематичних запитів

Після описання всіх категорій та встановлення рівнів ризику, проводять певні міри щодо їх зниження.

У результаті аналізу експертної системи COBRA можна дійти висновку, що аналіз ризиків, який буде здійснено даним методом, відповідає базовому рівню безпеки, тобто *рівень ризиків* не визначається, що і є основним недоліком для даного методу. Інтерфейс методу COBRA представлено на рис. 11.

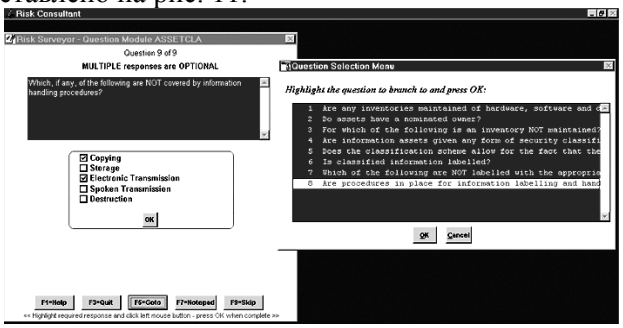

Рис. 11. Інтерфейс методу COBRA

Переваги методу COBRA:

- простота у використанні і, відносно, прийнятна вартість (усе залежить від бюджету, виділеного на ІБ) — $ 895 і $ 1995 за систему з модулем аналізу ризиків базового рівня.

До недоліків COBRA можна віднести:

- знання спеціальних електронних баз знань та процедур логічного виводу;
- застарілий, не дуже зручний для користувача інтерфейс;
- не визначається рівень ризиків, а лише базовий рівень безпеки;
- відсутність підтримки української та російської мов;
- виникають проблеми з генерацією звіту та можлива нестабільна робота під Win2000.

OCTAVE. Зміст методу OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх робіт.

Метод OCTAVE передбачає три фази аналізу ризиків:

1. Розробка профілю загроз, пов’язаних з активом.

2. Ідентифікація інфраструктурних уразливостей.

3. Розробка стратегії та планів безпеки.

Цей метод пропонує скласти профіль загроз та дерево варіантів. Профіль загрози включає в себе вказівки на актив (asset), тип доступу до активу (access), джерело загрози (actor), тип порушення або мотив (motive), результат (outcome) і посилання на описи загрози в загальнодоступних каталогах [3, с. 133].

Методика OCTAVE пропонує при описі профілю використовувати «дерево варіантів», приклад подібного дерева представлено на рис. 12.

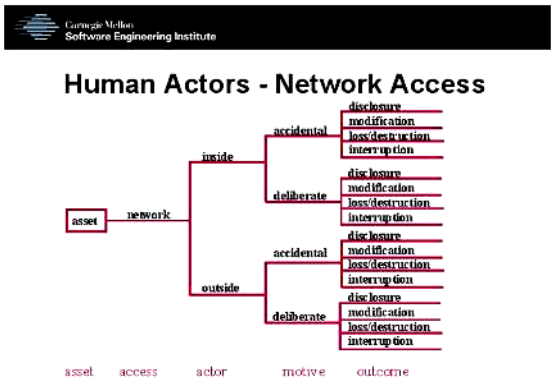

Рис. 12. Дерево варіантів,
що використовується при описі профілю

Профіль загроз містить інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки [3, с. 131].

Відповідно до аналізу методики OCTAVE можна дійти до висновку, що дану експертну систему широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками ІБ в ІТС.

Етапи аналізу ризику за методикою OCTAVE представлено на рис. 13 [6, с. 63].

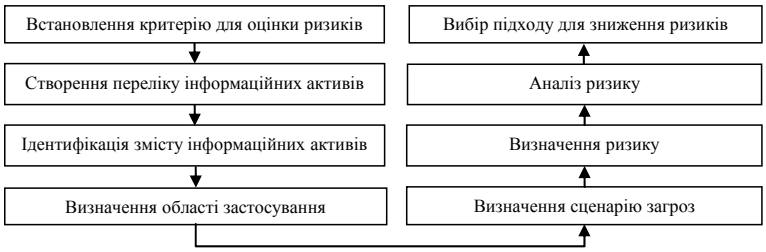

Рис. 13. Етапи аналізу ризику за методом OCTAVE [3, с. 131]

Переваги методу OCTAVE:

- швидко впроваджується;
- можливе застосування для організацій різного розміру та галузей застосування;
- високий рівень гнучкості.

До недоліків OCTAVE можна віднести:

- відсутність надання кількісної оцінки ризиків;
- припускає використання способів зниження ризиків і прийняття рішення;
- не спрямований на специфіку банківської сфери.

Існують різні OCTAVE методи, засновані на OCTAVE критеріях: OCTAVE, OCTAVE-S і OCTAVE Allegro. Інтерфейс методу OCTAVE представлено на рис. 13.

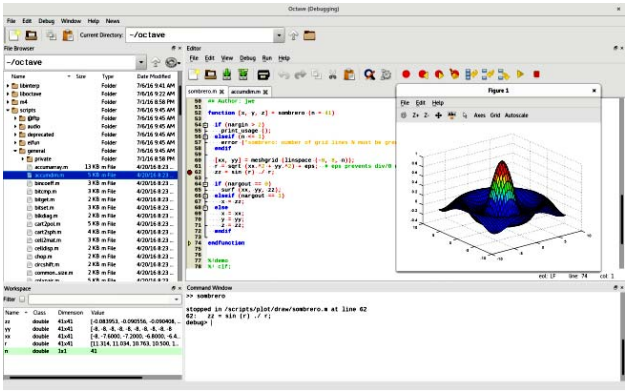

Рис. 13. Інтерфейс методу OCTAVE

Відмінністю методу OCTAVE від вище переглянутих є те, що при оцінці ризику дана експертна система дає тільки оцінку очікуваного збитку, без оцінки вірогідності. А також загальнодоступною та безкоштовною є вся документація по OCTAVE. Сьогодні існують окремі нормативно-правові документи, які регламентують питання ІБ, як основу для створення методів оцінювання інформаційних ризиків в ІТС [3].

Більшість програмних експертних систем відповідають міжнародному стандарту ISO/IEC 27001:2005. Відповідні Міжнародні стандарти визначають вимоги до СУІБ, управління ризиками, метрики і вимірювання, а також керівництво з впровадження [13, 8, с. 54].

Ключовою моделлю, що використовується у сфері управління ризиками інформаційної безпеки (УРІБ) модель, що знайшла відображення в усіх стандартних підходах до УРІБ і являє собою основу ISO/IEC 27005 і BS 7799-3 [13, 8, с. 55].

Дана модель дає перелік і послідовність таких необхідних для управління ризиками ІБ процесів, як планування, реалізація, перевірка, дія. Відповідно з даним стандартом документація, яка визначає управління інформаційними ризиками організації, повинна включати: документовану заяву про політику та цілі СУІБ; область програми СУІБ; процедури і засоби управління на підтримку СУІБ; опис методології оцінки ризиків; звіт про оцінки ризиків; план обробки ризиків [7, с. 199]. Цей стандарт підготовлений в якості моделі для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та покращення системи забезпечення інформаційної безпеки. Окрім вищезазначеного міжнародного стандарту існує ряд інших у галузі забезпечення ІБ в ІТС, розглянуті в табл. 1.

Таблиця 1

Міжнародні стандарти з керування методів для визначення інформаційних ризиків та їх коротка характеристика

Стандарт	Назва стандарту	Коротка характеристика
ISO/IEC 27002-2012	Інструкція з менеджменту інформаційної безпеки для телекомунікаційних організацій	Цей стандарт надає додаткові рекомендації з реалізації та менеджменту ІБ в телекомунікаційних організаціях. Визначає цілі, вимоги оцінки ризику до системи ІБ та забезпечує контроль управління. Діючий Міжнародний стандарт пропонує рекомендації та основні принципи введення, реалізацію, підтримку й поліпшення менеджменту ІБ
ISO/IEC 27003-2012	Інструкція з реалізації системи менеджменту ІБ	У цьому Міжнародному стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження в СМІБ відповідно зі стандартом ISO/IEC 27001:2005, який розглядає процес визначення та розробку СМІБ від початку до стану впровадження
ISO/IEC 27004-2011	Менеджмент інформаційної безпеки вимірювання	Цей стандарт містить рекомендації з розробки та використання вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої СМІБ. Процес вимірювання реалізується у вигляді програми, пов'язаний з ІБ. Програма вимірювань надає допомогу користувачу у виявленні і оцінюванні вимог, яким не відповідає процес ефективності контролю і управління СМІБ, а також визначення пріоритетів дій, спрямованих на удосконалення або зміну цих процесів
ISO/IEC 27005-2010	Менеджмент ризику інформаційної безпеки який конкретизує поняття інформаційного ризику	Цей стандарт поданий у вигляді додатку прикладу типових загроз, уразливостей та потреб інформаційної безпеки. Проблема оцінювання та дослідження інформаційних ризиків насамперед асоціюється з британським стандартом BS 7799, а саме з його двома частинами: першою — BS 7799-1 «Звіт правил з менеджменту безпеки інформації» та другою — BS 7799-2 «Системи менеджменту безпекою інформації», у яких вперше питання аналізу стану безпеки інформації та формування її захисту були напряму пов'язані з інформаційними ризиками. Однак, безпосередньо, аспекти оцінювання та управління ризиками були докладніше розглянуті у третій частині стандарту BS 7799-3 «Настанови з менеджменту ризиками безпеки інформації»
ISO/IEC TR 13335-2:1997	Настанови з керування безпекою інформаційних технологій (IT)	Надати рекомендації, а не конкретні рішення з керування безпекою інформаційних технологій (IT). Кваліфікація осіб, відповідальних за безпеку IT у межах організацій повинна бути достатньою для адаптування матеріалів, поданих у цьому стандарті, до конкретних потреб організацій

Аналізуючи основні міжнародні стандарти BS 7799-3 та ISO/IEC 27005, стає очевидним, що вони визначають усі найважливіші аспекти, пов'язані з інформаційними ризиками. Це стосується процесної моделі, елементів управління ризиками, підходів до аналізу ризиків, способам їх обробки тощо. Стандарт BS 7799-3 допускає використання, як якісних, так і кількісних методів оцінки ризику. Характерною рисою цього стандарту є принцип усвідомленості процесів оцінювання, оброблення, контролю та оптимізації ризиків в організації [11, 8, с. 55]. Результати порівняльного аналізу основних експертних систем для оцінювання ризиків наведено в табл. 2.

Таблиця 2

Порівняльний аналіз інструментальних засобів оцінювання ризиків

Критерії порівняння	CRAMM	Risk Watch	ГРИФ 2006	NIST	COBRA	OCTAVE
Відповідність стандартам ISO 2700x	+	+	+	+	+	+
Оцінка захищеності	+	+	+	+	+	+
Швидкодія	+	–	+	–	+	+
Облік послідовності контрзаходів при розрахунку ризиків	+	–	+	+	+	–

Закінчення табл. 2

Критерії порівняння	CRAMM	Risk Watch	ГРИФ 2006	NIST	COBRA	OCTAVE
Визначення рівня ризиків для різних моделей ІТС	+	–	+	–	+	–
Можливість завдання власних контрзаходів	+	+	–	–	+	–
Оцінка аналізу ризиків	Змішана	Кількісна	Змішана	Змішана	Якісна	Якісна
Наявність ліцензії	+	+	+	+	+	+
Вартість	2000–5000 дол. США	Від 15 000 дол. США	Від 1000 дол. США	149–254 дол. США	7200–16 000 грн.	Від 2000 дол. США
Зручність інтерфейсу	Не зручний	Не зручний	Зручний	Не зручний	Зручний	Зручний
Необхідність спеціальної підготовки для роботи з засобами	+	+	+	+	–	–
Складність визначення ризику	Складна	Складна	Не дуже складна	Не дуже складна	Не дуже складна	Не складна
Оперативність визначення ризику	+	–	+	–	+	+

Зробивши порівняльний аналіз інструментальних засобів оцінювання ризиків, визначимо найбільш поширені недоліки, до яких відносять:

1. Складність отримання даних. Дані необхідно оцінювати безперервно на достатньо великому проміжку часу.

2. Постійне оновлення програмного забезпечення призводить до досить частої зміни інформаційного середовища.

3. Час, який витрачається для проведення аналізу, може не відповідати з точки зору оперативності реагування на швидкозмінні засоби інформаційної безпеки.

Щодо кількісних методів оцінювання інформаційних ризиків можемо зробити висновки про те, що вони є не точними та не надійними з певних причин:

1. Для кількісної оцінки складно зібрати дані у зв'язку з необхідністю їх точної реєстрації за навіть великий період.

2. Сучасне інформаційне середовище часто може змінюватися через постійне вдосконалення програмного забезпечення.

3. Витрати часу для аналізу досить великі.

Основні результати

До основних результатів автори статті відносять узагальнення аналізу інструментальних засобів оцінювання ризиків ІБ.

Визначення основних недоліків, які присутні в цих засобах.

Це дає можливість у розробці та впровадженні в Україні власного інструментального засобу оцінювання ризиків ІБ оптимального за якістю та ціною і який би не суперечив міжнародним стандартам.

Висновки

Проведений аналіз існуючих методів визначення ризиків інформаційної безпеки в ІТС та сучасних міжнародних стандартів, які регламентують питання ІБ свідчить проте, що характерною основою експертних систем оцінювання ризиків є ймовірність виникнення тієї чи іншої події, яка впливає на ймовірність реалізації загрози. Для точного визначення рівня ризиків ІБ необхідно мати додаткову інформацію, яка отримується в результаті проведення ряду ретельних досліджень, обробка яких здійснюється у більшості експертними методами.

ЛІТЕРАТУРА

1. **Юдін О. К**. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О. К. Юдін, С. С. Бучик. — К. : НАУ, 2015. — 213 с.

2. **Чунарьова А. В**. Аналіз підходів та програмних рішень оцінки і контролю інформаційних ризиків в комп'ютеризованих системах / А. В. Чунарьова, І. І. Пархоменко, І. І. Сащук // Вісник Інженерної академії України. — Х. — 2014. — Вип. 2. — С. 138–142.

3. **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. — Л. : Академія сухопутних військ імені гетьмана Петра Сагайдачного, 2014. — Вип. 8 (124).— ISSN 1681–7710. — С. 128–134.

4. **Бучик С. С**. Методика оцінювання інформаційних ризиків в автоматизованій системі /

С. С. Бучик, С. В. Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. — Житомир: ЖВІ ДУТ, 2015. — Вип. 11. — С. 33–43.

5. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут, О. К. Климович // Системи обробки інформації. — Л. : Академія сухопутних військ імені гетьмана Петра Сагайдачного, 2015. — Вип. 3 (128). — ISSN 1681-7710. — С. 75–79.

6. **Корнієнко Б. Я**. Прикладні програми управління інформаційними ризиками / Б. Я. Корнієнко, Ю. О. Максімов, Н. М. Марутовська // Захист інформації. — К. : Науково-практичний журнал, 2012. — Вип. 4. — С. 60–64.

7. **Астахов А. М**. Искусство управления информационными рисками / А. М. Астахов. — М. : ДМК Пресс, 2010. — 312 с.

8. **Замула О. А**. Аналіз міжнародних стандартів у галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації. — Х. : Харківський національний університет радіоелектроніки, 2011. — Вип. 2 (92). — ISSN 1681-7710. — С. 53–55.

9. **Петренко С. А**. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. — М. : Компания АйТи ; ДМК Пресс, 2004. — 384 с.

10. **Сергей Петренко**. Методики и технологии управления информационными рисками / Сергей Петренко, Сергей Симонов [Електронный ресурс]. — Режим доступу: http://citforum.ru/security/articles/risk/

11. **Куканова Наталья**. Современные методы и средства анализа и управление рисками информационных систем компаний / Наталья Куканова [Електронний ресурс]. — Режим доступу: http://dsec.ru/ipm-research-center/article/ modern_ methods_and_ means_for_analysis_and_risk_ management_ of_information_systems_of_companies

12. **Домарев В. В**. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев // — К. : ТИД Диасофт, 202. — С. 423–436.

13. Information technology — Security techniques–Information security risk management: ISO/IEC 27005 : 2008 [Електронний ресурс]. — Режим доступу: http: /www.iso.org/iso/catalogue_detail?csnumber=42107.

Бучик С. С., Шалаєв В. О.

АНАЛІЗ ІНСТРУМЕНТАЛЬНИХ МЕТОДІВ ВИЗНАЧЕННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

У статті визначено мету, напрямок та завдання проведення аналізу основних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем. В основу системи інформаційної безпеки інформаційно-телекомунікаційної системи покладено процес управління ризиками, який включає в себе такі основні процеси, як аналіз та оцінювання. На сьогоднішній день існує велика кількість методів оцінювання та засобів управління інформаційними ризиками. У даній статті розглянуто застосування експертних систем, які проводять більш високу оцінку ризиків інформаційної безпеки для різних моделей інформаційно-телекомунікаційних систем та уникають порушень забезпечення конфіденційності, цілісності та доступності інформації. Проведено аналіз роботи методів щодо формування звітності та причин виникнення ризиків з економічною ефективністю можливих контрзаходів. Розглядаються основні етапи оцінювання та зниження інформаційних ризиків у системах інформаційної інфраструктури. Проаналізовано процедуру оцінювання інформаційних ризиків згідно основних міжнародних стандартів.

Ключові слова: інформаційно-телекомунікаційна система; інформаційна безпека; ризик; система управління інформаційної безпеки; інформаційна безпека інформаційно-телекомунікаційної системи; управління ризиками інформаційної безпеки.

Бучик С. С., Шалаев В. А.

АНАЛИЗ ИНСТРУМЕНТАЛЬНЫХ МЕТОДОВ ОПРЕДЕЛЕНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

В статье определены цель, направление и задачи по анализу основных методов определения рисков информационной безопасности информационно-телекоммуникационных систем. В основу системы информационной безопасности информационно-телекоммуникационной системы положен процесс управления рисками, который включает в себя такие основные процессы, как анализ и оценивание. На сегодняшний день существует большое количество методов оценки и средств управления информационными рисками. В данной статье рассмотрено применение экспертных систем, которые проводят более высокую оценку рисков информационной безопасности для разных моделей информационно-телекоммуникационных систем и избегают нарушений конфиденциальности, целостности и доступности информации. Проведен анализ методов работы по формированию отчетности и причин возникновения рисков с экономической эффективностью возможных контр-

мер. Рассматриваются основные этапы оценки и снижения информационных рисков в системах информационной инфраструктуры. Проанализирована процедура оценивания информационных рисков на основе международных стандартов.

Ключевые слова: информационно-телекоммуникационная система; информационная безопасность; риск; система управления информационной безопасности; информационная безопасность информационно-телекоммуникационной системы; управление рисками информационной безопасности.

Buchyk S. S., Shalaev V. A.

THE ANALYSIS INSTRUMENTAL METHODS OF IDENTIFICATION OF RISKS OF INFORMATION SECURITY INFORMATION AND TELECOMMUNICATION SYSTEMS

The article defines the purpose, direction and objectives of analysis of the main methods of identification of risks of information security information and telecommunication systems. The basis of the system of information security in information and telecommunication systems is based on the risk management process, which involves such main processes as analysis and evaluation. There are a large numbers of assessment methods and tools of information risk management nowadays. This article describes the application of expert systems, which hold a higher risk assessment of information security for different models of information and telecommunication systems and help to avoid violations of the confidentiality, integrity and availability of information. The analysis of the working methods of reporting and the reasons for the occurrence of risks with the economic effectiveness of possible countermeasures is made. The main stages of the assessment and mitigation of information risks in the information infrastructure systems are considered. The procedure of assessment of information risks in accordance with basic international standards is analyzed.

Keywords: information-telecommunication system; information security; risk; management system of information security; information security in information and telecommunication systems; management of information security risks.

Стаття надійшла до редакції 15.08.2017 р.
Прийнято до друку 01.09.2017 р.
Рецензент – д-р техн. наук, проф. Юдін О. К.