УДК 621.941-229.3:531.133

Ковальчук П.Р., аспірант
Морозова І.В.,канд. техн. наук, доцент
Національний авіаційний університет, м. Київ, kovallarm@gmail.com

ОЦІНЮВАННЯ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В СИСТЕМАХ ТЕЛЕКОМУНІКАЦІЙ: РІЗНОМАНІТНІ МЕТОДИ

Актуальність та необхідність застосування процедур оцінки та управління загрозами та ризиками ІБ неухильно зростає у зв'язку з підвищенням ролі інформаційно-телекомунікаційних систем (ІТС) та технологій у процесах функціонування організацій як суб'єктів господарювання. При цьому, як правило, основна увага приділяється вимогам та рекомендаціям відповідної Української нормативно-методичної бази у галузі захисту інформації (ЗІ).

Практично всі існуючі програмні реалізації підходів до оцінки загроз ІБ ІТС не враховують методики, що містяться у вітчизняних або міжнародних стандартах ІБ ІТС. Що не дозволяє їх використовувати в практичних завданнях повсякденної діяльності фахівців у галузі ІБ ІТС. Оцінювання ризиків полягає у визначенні кількісних та якісних показників, формуванні реєстру ризиків та ранжируванні ризиків.

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.

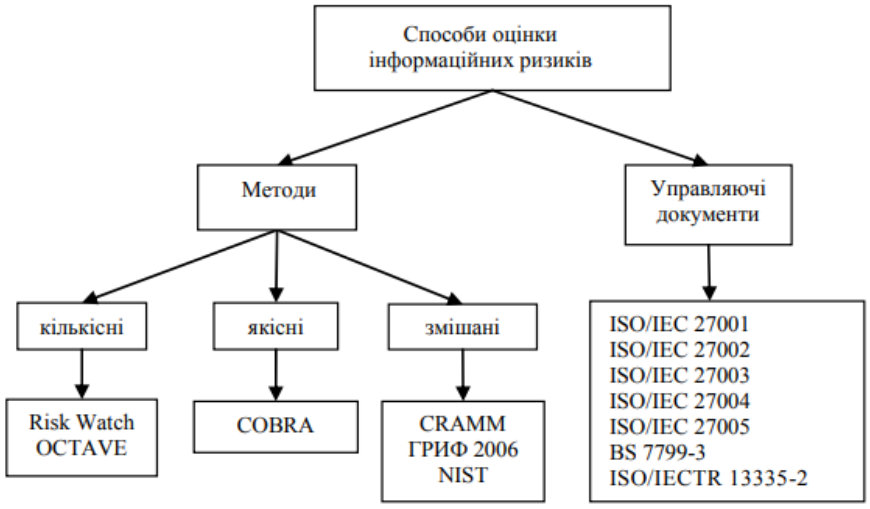

Рис. 1 – Схема інструментальних методів визначення ризиків інформаційної безпеки в ІТС

Метод CRAMM пропонує всі процедури методу поділити на три послідовних етапи, які розглянуто на рис. 2.

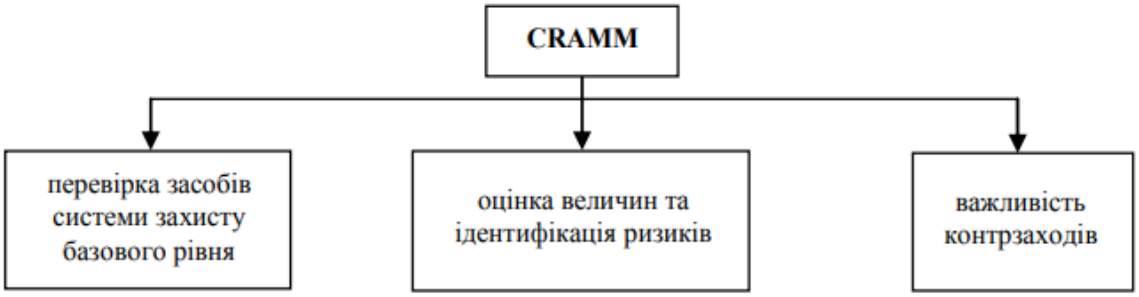

Рис. 2 – Етапи проведення аналізу ризиків ІБ методом CRAMM

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. 3.

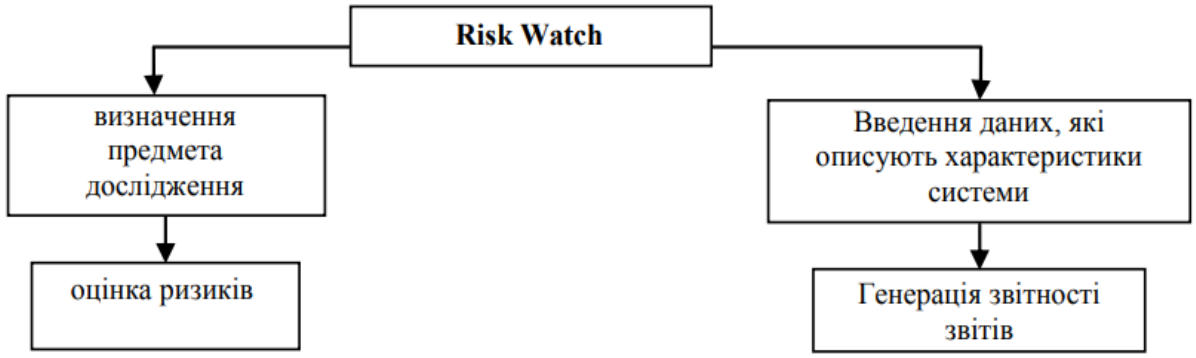

Рис. 3. Етапи проведення аналізу ризиків ІБ методом Risk Watch

Аналіз оцінювання ризиків на основі тематичних запитів проводиться за наступними категоріям, які розглянуто на рис. 4.

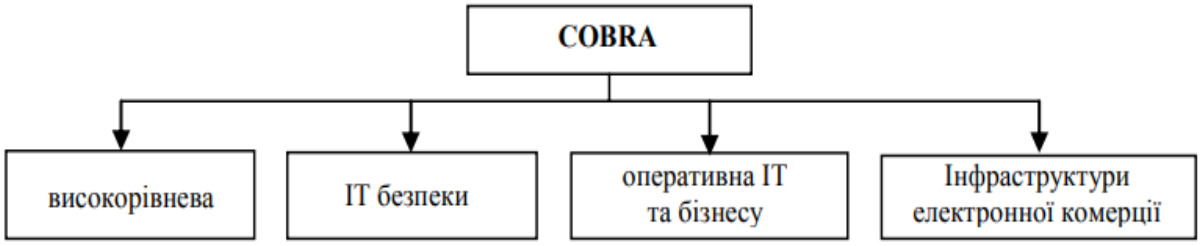

Рис. 4. Етапи оцінювання ризиків на основі тематичних запитів

Зростання ролі інформаційно-телекомунікаційних систем (ІТС) та технологій у процесах функціонування організацій робить організацію режиму інформаційної безпеки критично важливим стратегічним фактором розвитку будь-якої вітчизняної компанії. Однак, на даний момент багато провідних вітчизняних компаній не використовують додаткові ініціативи з захисту інформації, спрямовані на забезпечення стійкості та стабільності функціонування корпоративних ІТС для підтримки безперервності бізнесу в цілому. Правильна оцінка загроз ІБ ІТС та виявлення серед них найактуальніших є основою для побудови надійної системи захисту інформації. Проте, експертні групи, які визначають ймовірності реалізації загроз ІБ ІТС, не завжди застосовуються на конкретних підприємствах та в організаціях. Прогнозування загроз ІБ ІТС часто взагалі не виконується, тоді як існуючі програмні реалізації підходів до оцінки загроз ІБ ІТС не враховують методики, що містяться у вітчизняних або міжнародних стандартах ІБ ІТС, що не дозволяє їх використовувати в практичних завданнях повсякденної діяльності фахівців у галузі ІБ ІТС. Таким чином, оцінка та управління загрозами та ризиками ІБ є необхідною умовою для створення надійної системи захисту інформації.

Список посилань

1. Хмелевський Р. Дослідження оцінки загрози інформаційної безпеки об’єктів інформаційної діяльності / Р. Хмелевський // Сучасний захист інформації. – 2016. – №4. – с. 65–70.

2. Черниш В. Методика оцінки інформаційних ризиків з використанням методу аналізу ієрархії / В. Черниш // Радіоелектронні і комп'ютерні системи. – 2012. – №1. – pp. 46-50.

3. Домарьов В.В. Безпека інформаційних технологій. Системний підхід / В.В. Домарьов. – К.: ТОВ ТІД «Діасофт», 2004.

4. Корнієнко Б. Я. Прикладні програми управління інформаційними ризиками / Б. Я. Корнієнко, Ю. О. Максімов, Н. М. Марутовська // Захист інформації. – 2012. – Вип. 4. – С. 60–64.