УДК 004.056.32

Корнієнко Б.Я., Максімов Ю.О., Марутовська Н.М.

ПРИКЛАДНІ ПРОГРАМИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

В статті 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.

Ключові слова: інформаційний ризик, прикладні програми, якісні методики, кількісні методики, управління ризиками.

Вступ. У сучасних умовах одне з актуальних практичних завдань - оцінка ефективності заходів щодо захисту інформації в інформаційних комп'ютерних системах. Дослідження цього завдання дасть можливість розробникам і власникам інформаційних комп'ютерних систем одержувати обґрунтовану оцінку техніко-економічної доцільності різних заходів і способів захисту інформації та формувати раціональний комплекс заходів для забезпечення інформаційної безпеки, економно витрачаючи виділені на ці цілі ресурси.

Актуальність. Сьогодні не викликає сумнівів необхідність інвестицій в забезпечення інформаційної безпеки сучасних інформаційно-комунікаційних систем. Основне питання сучасного бізнесу - як оцінити необхідний рівень витрат на інформаційну безпеку для забезпечення максимальної ефективності інвестицій в дану сферу. Для вирішення цього питання існує тільки один спосіб - застосовувати комплекси аналізу ризиків, що дозволяють оцінити існуючі в системі ризики і вибрати оптимальний по ефективності варіант захисту.

Постановка задачі. У даній статті описується методика аналізу інформаційних ризиків з використанням певних програмних комплексів, що дозволяє оцінити ефективність використовуваних технологій захисту інформації для трьох граней інформаційної безпеки: конфіденційність, цілісності та доступності.

Викладення матеріалу. Якісні методики управління ризиками прийняті на озброєння в технологічно розвинених країнах численною армією внутрішніх і зовнішніх IT-аудиторів. Ці методики досить популярні і відносно прості, і розроблені, як правило, на основі вимог міжнародного стандарту ISO 17799:2002. До якісних методиках управління ризиками на основі вимог ISO 17999 відносяться методики Risk Advisor, COBRA, КОНДОР+, Proteus Enterprise.

Risk Advisor. Це інструментарій аналітика або менеджера в галузі інформаційної безпеки[1]. Реалізована методика, що дозволяє задати модель інформаційної системи з позиції інформаційної безпеки, ідентифікувати ризики, загрози, втрати в результаті інцидентів. Основними етапами роботи є: опис контексту, визначення ризиків, оцінка загроз та можливої шкоди, вироблення керуючих впливів і розробка плану відновлення і дій у надзвичайних ситуаціях.

На етапі опису контексту описується модель взаємодії організації із зовнішнім світом в декількох аспектах: стратегічному, організаційному, бізнес-цілі, управління ризиками, критерії. Стратегічний аспект описує сильні і слабкі сторони організації із зовнішніх позицій, варіанти розвитку, класи загроз і відносини з партнерами. Організаційний контекст описує відносини всередині організації: стратегію, цілі на організаційному рівні, внутрішню політику. Контекст управління ризиками описує концепцію інформаційної безпеки. Критерії оцінки - критерії оцінки, використовувані при управлінні ризиками. Для описів ризиків задається матриця на основі деякого шаблону.

Ризики оцінюються по якісній шкалі і розділяються на прийнятні і неприйнятні. Потім обирають управляючі дії з урахуванням зафіксованої раніше системи критеріїв, ефективності контрзаходів і їх вартості. Вартість і ефективність також оцінюються в якісних шкалах.

Загрози певним чином класифікуються, потім описується зв'язок між ризиками і загрозами. Опис також робиться на якісному рівні і дозволяє зафіксувати їх взаємозв'язки.

Для втрат описуються події, пов'язані з порушенням режиму інформаційної безпеки. Втрати оцінюються в обраній системі критеріїв. У аналізі результатів сформується докладний звіт у вигляді графа ризиків.

Сильною стороною розглянутої методики є можливість опису різних зв'язків, адекватний облік багатьох факторів ризику та суттєво менша трудомісткість в порівнянні з CRAMM.

До недоліків цих методик наступне: використання методик вимагає спеціальної підготовки і високої кваліфікації аудитора; програмний інструментарій генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці; не дозволяє створювати власні шаблони звітів або модифікувати наявні; можливість внесення доповнень в базу знань не доступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретної організації; ПЗ існує тільки на англійській мові; висока вартість ліцензії.

COBRA (Consultative Objective and Bi-Functional Risk Analysis). У другій половині 90х років компанія C & A Systems Security Ltd. розробила методику і відповідний інструментарій для аналізу і управління інформаційними ризиками під назвою COBRA[1]. Ця методика дозволяє виконати в автоматизованому режимі найпростіший варіант оцінювання інформаційних ризиків будь-якої компанії. Для цього пропонується використовувати спеціальні електронні бази знань і процедури логічного висновку, орієнтовані на вимоги ISO 17799. Методика COBRA використовує вимоги стандарту ISO 17799 у вигляді тематичних анкет, на які слід відповісти в ході оцінки ризиків інформаційних активів та електронних бізнес-транзакцій компанії (рис.1) Далі введені відповіді автоматично обробляються, і за допомогою відповідних правил логічного висновку формується підсумковий звіт с поточними оцінками інформаційних ризиків компанії та рекомендаціями щодо їх управління.

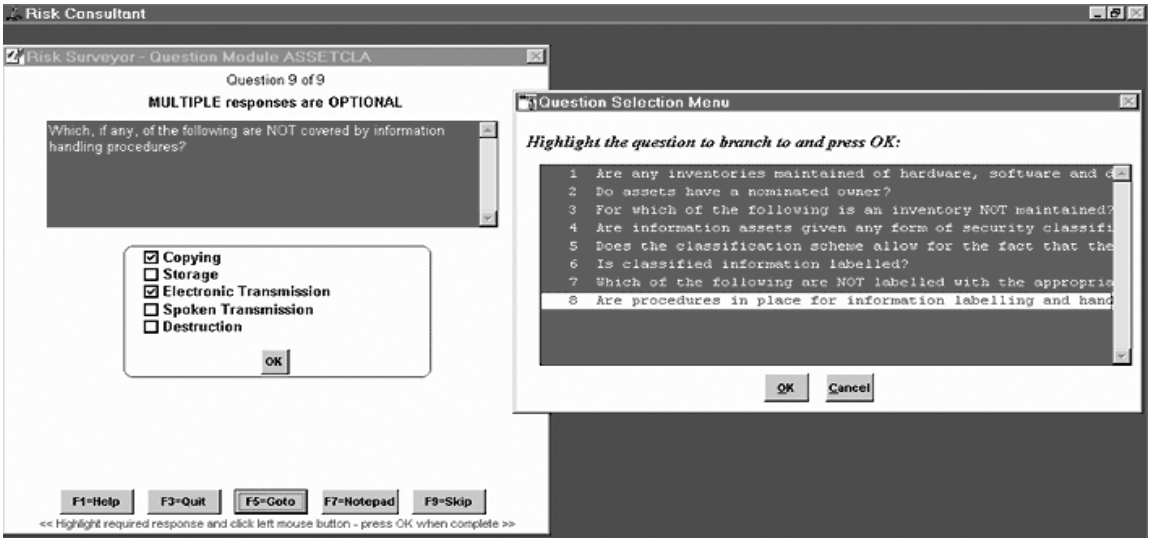

Рис. 1. Методика аналізу і управління інформаційними ризиками COBRA

КОНДОР. Продукт дозволяє фахівцям перевірити політику інформаційної безпеки компанії на відповідність вимогам ISO 17799. КОНДОР включає в себе більше 200 питань, відповівши на які фахівець отримує докладний звіт про стан існуючої політики безпеки, а також модуль оцінки рівня ризиків відповідності вимогам ISO 17799 (рис.2). У звіті відображаються всі положення політики безпеки, які відповідають і не відповідають стандарту, а також існуючий рівень ризику невиконання вимог політики безпеки відповідно до стандарту. Елементам, які не виконуються, даються коментарі та рекомендації експертів. За бажанням фахівця, який працює з програмою, можуть бути вибрані генерація звіту, наприклад, за якимось одним або декількома розділами стандарту ISO 17799, загальний

докладний звіт із коментарями, загальний звіт про стан політики безпеки без коментарів для керівництва. Всі варіанти звітів для більшої наочності супроводжуються діаграмами. КОНДОР дає можливість фахівцеві відстежувати внесені на основі виданих рекомендацій зміни в політику безпеки, поступово приводячи її у повну відповідність до вимог стандарту. Дана система реалізує метод якісної оцінки ризиків за рівневої шкалою ризиків: високий, середній, низький.

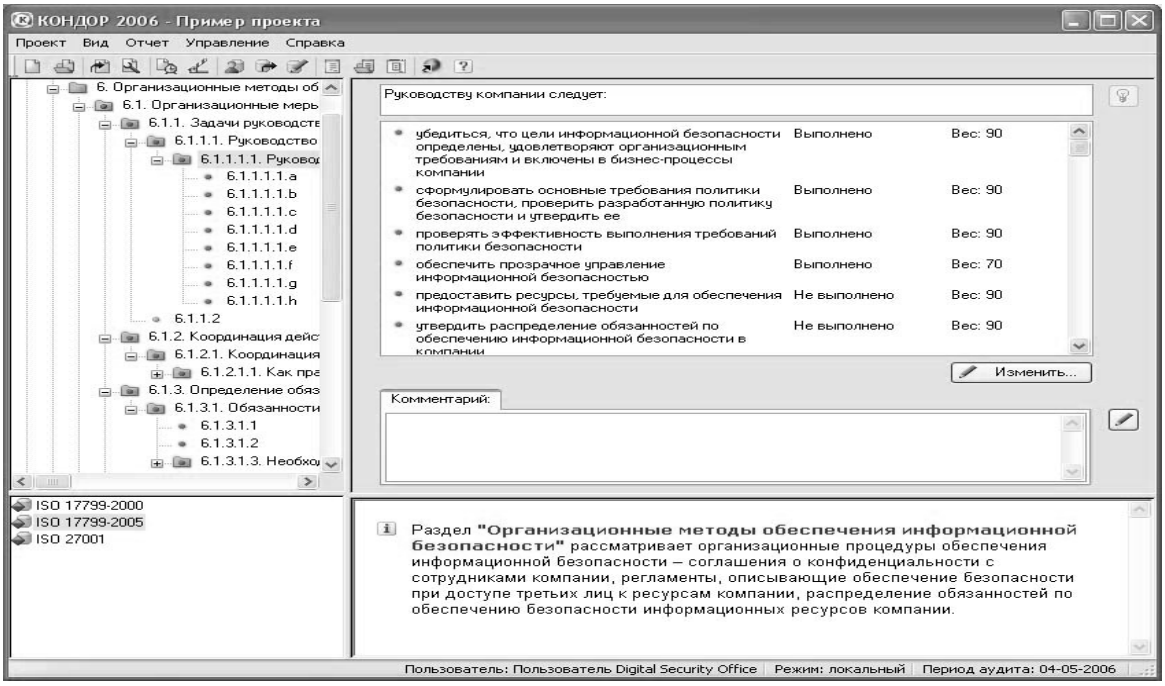

Рис. 2. Методика оцінювання інформаційних ризиків КОНДОР

Proteus Enterprise. Proteus - потужна система для підтримки процесів системи управління інформаційною безпекою, що включає в себе засоби контролю відповідності, оцінки впливу на бізнес, оцінки ризиків, управління безперервністю бізнесу, управління інцидентами, управління активами та організаційними ролями, а також репозитарій політик і засоби планування [1, 2]. Контроль відповідності підтримує будь-які стандарти (міжнародні, галузеві та корпоративні) і поставляється разом з набором шаблонів анкет. Всі дії, зроблені в системі, реєструються в журналі аудиту.

Система дозволяє проводити онлайн-аудити у внутрішніх підрозділах і у зовнішніх постачальників. Запезпеченна повна підтримка стандартів BS ISO/IEC 27001, BS ISO/IEC 17799, PCI, ISF SOGP, NIST Combined Code, Sarbanes Oxley, GLB, Data Protection Act, Freedom of Information Act, Caldicott, Basel II, BS25999, Civil Contingency Bill.

Proteus RiskView надає інформацію про корпоративне управління, відповідні вимоги та ризики для керівництва в реальному часі в графічній формі (рис. 3). Потужні засоби генерації звітів на основі Business Objects. Другу групу методик управління ризиками складають кількісні методики, актуальність яких обумовлена потребою вирішення різних оптимізаційних задач, які часто виникають у реальному житті. Для вирішення завдань і розробляються методи і методики кількісної оцінки і управління ризиками на основі структурних і рідше об'єктно-орієнтованих методів системного аналізу і проектування (SSADM - Structured Systems Analysis and Design).

Популярними програмними комплексами цієї групи управління ризиками є: RiskWatch, CRAMM, Система ГРИФ. Ці системи є типовими ефективними комплексами кількісного підходу оцінки та управління інформаційними ризиками про які є достатня кількість аналітичного матеріалу. Розглянемо новий продукт інформаційної безпеки BCM-Analyser.

BCM-Analyser. Це принципово новий комплекс, що володіє унікальним механізмом оптимізації ризиків і вироблення стратегії забезпечення безперервності бізнесу. Даний продукт характеризується відкритістю математичних методів, універсальністю підходів до завдання способів і засобів обробки ризиків, можливістю внесення будь-яких змін у параметри комплексу, механізмом автоматичного вибору оптимальних заходів обробки ризиків (рис. 4).

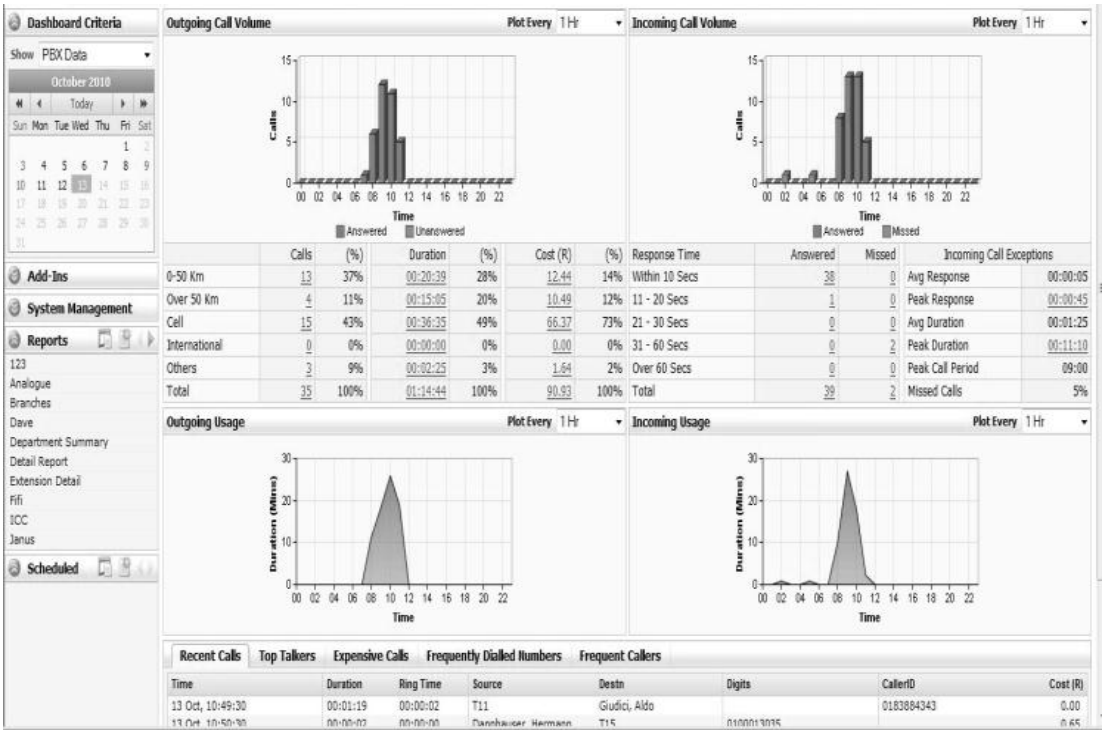

Рис. 3. Управління інформаційною безпекою за допомогою Proteus Enterprise

Основою для аналізу безперервності бізнес-процесів є виявлення бізнес-процесів і об'єктів безпеки або активів (приміщень, машин, устаткування, обчислювальної техніки, конкретних файлів, каталогів, баз даних, персоналу та інших ресурсів), що забезпечують функціонування цих бізнес-процесів. У програмному комплексі можливе завдання будь-яких об'єктів [3]. Ключовими відмінностями BCM-Analyser у порівнянні з аналогічними розробками є:

- повністю автоматична система. Ґрунтуючись на характеристиках компонентів беруть участь у бізнес процесах організації, система видає єдиний найбільш оптимальний варіант побудови системи захисту від ризиків - варіант з найменшими очікуваними витратами для бізнесу;
- продукт, орієнтований на бізнес, що володіє розвиненими механізмами врахування всіляких витрат пов'язаних з впровадженням системи захисту, як капітальних (CAPEX), так і операційних (OPEX);
- володіє уніфікованим механізмом опису будь-яких контрзаходів, залежностей між ними, що дозволяє врахувати будь-які способи, механізми, процеси реалізовує якусь стратегію управління ризиками.

Функціональні можливості BCM-Analyser: можливості введення даних про компоненти бізнес процесів, їх властивості, загрози, контрзаходи і залежностях між ними; завдання очікуваного збитку компонентів бізнес процесів у вигляді функції, що враховує зміну збитку з часом; гнучкі можливості за завданням різноманітних вартісних, функціональних, часових характеристик контрзаходів; більше 100 заздалегідь заданих контрзаходів; можливість визначення необмеженої кількості контрзаходів; автоматичний перебір можливих варіантів побудови системи захисту з вибором оптимального, що дає мінімальне значення суми вартостей залишкових ризиків та збитків, вартості експлуатації;

можливість розрахунку вартості захисту на довільну кількість років, що дозволяє більш точно врахувати вартість експлуатації в загальній вартості системи захисту; складний алгоритм оптимізації, що дає максимально ефективний варіант системи захисту навіть при великих вибірках контрзаходів; збереження та експорт результатів розрахунків в формати файлів Excel і txt; клієнт-серверна архітектура, що дозволяє працювати в багатокористувацькому режимі.

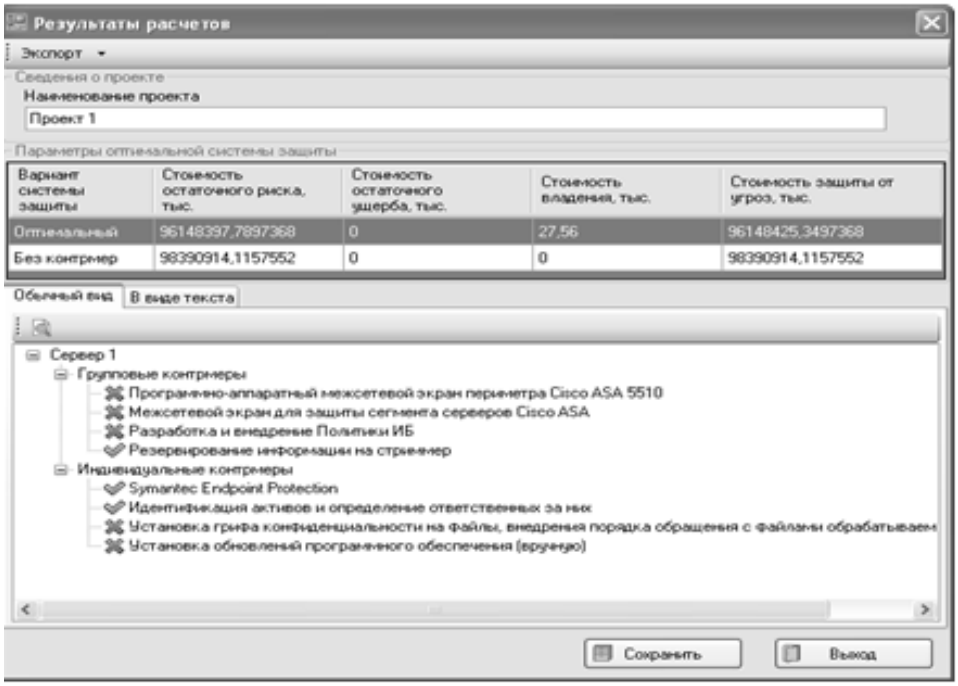

Рис. 4. Автоматична система BCM-Analyser

Висновок. Отже, на ринку інформаційних технологій існує велика кількість програмних засобів впровадження яких забезпечує гідне керування інформаційними потоками та виявлення інформаційно – технологічних ризиків пов'язані з діяльністю організації для якої застосовуються ті чи інші методи. Усі програми можна розділити на дві великі групи: програми, що застосовуються якісну та кількісну оцінку ризиків. Є комплекси, що об'єднують ці два підходи наприклад Digital Security Office, РискМенеджер, Oracle Crystal Ball, @Risk, але для більшої надійності потрібно чітко оцінити потреби організації виходячи із сфери їх діяльності та здійснювати вибір необхідного програмного забезпечення.

ЛІТЕРАТУРА

1. Proteus® Enterprise. // infogov.co.uk: сайт компанії «InfoGov» 2012.URL: http:// infogov.co.uk.
2. Программные продукты для анализа рисков. // iso27000.ru: русскоязычный информационный портал, посвященный вопросам управления информационной безопасностью 2012.URL: http:// iso27000.ru.
3. BCM-Analyser. // iradd.ru: сайт компанії «IRADD» 2012.URL: http:// iradd.ru.ru.

Надійшла: 19.10.2012 р.

Рецензент: д.т.н., професор Юдін О.К.

УДК 004.056.5(045)

Пархоменко І.І., Воскобойніков А.О.

ЗАХИСТ WEB-РЕСУРСІВ ВІД АТАК ТИПУ COMMAND EXECUTION

В статті розглянуто принцип забезпечення захисту web-сайту від атак command execution, а саме від SQL-ін'єкцій та XSS, доведено небезпечність даних атак та наведені можливі наслідки, до яких вони можуть призвести. Запропоновано варіант захисту від command execution через фільтрацію вхідних даних.

Ключові слова: атака виконання коду, SQL-ін'єкція, міжсайтовий скриптинг, безпека веб-сайту