УДК 004.056.5

ПРИКЛАДНІ АСПЕКТИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Петренко Т.А., викладач кафедри математичного моделювання та інформатики
Чернігівського державного технологічного університет

Висока інформатизація сучасного підприємства - невід'ємний елемент його успіху. Надаючи своїм користувачам велику конкурентну перевагу, інформаційні технології одночасно висувають і додаткові вимоги. Головною з них, безперечно, є вимога до інформаційної безпеки та захисту інформації. [1] Очевидно, що забезпечення безпеки конфіденційної інформації - не тільки частина управління ризиками, але і фундаментальний елемент ведення бізнесу.

При аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати її специфіку, яка полягає в тому, що вона є складовою частиною інформаційних технологій - області, що розвивається безпрецедентно високими темпами. [2]

На сьогоднішній день велика кількість різнопланових нормативних документів і публікацій ускладнює процес прийняття конкретних рішень з ефективного захисту інформаційних ресурсів в багатьох організаціях. Недостатня кваліфікація спеціалістів або їх відсутність призводить до хаотичного руху інформаційних потоків, які відстежують випадкові люди.

Найчастіше основна роль відводиться системному адміністратору, який за своєю освітою хоч і є висококваліфікованим фахівцем з сучасних комп'ютерних технологій, але все ж таки захист інформації не є його основним напрямом діяльності. Керівники організацій не завжди ставлять перед ним конкретні завдання з контролю автоматизованих систем на предмет наявності конфіденційної інформації у відкритому доступі, розмежуванню доступу співробітників. Все це створює передумови до витоку інформації.

На сьогоднішній день назріла ситуація, коли необхідно шукати нові підходи до вирішення завдань ефективного захисту інформації на місцях, яку може забезпечити тільки фахівець, який має в своєму арсеналі більш досконалу нормативно-правову базу, достатню кількість методичних прийомів захисту, а також необхідні повноваження в рамках посадових обов'язків. В області інформаційної безпеки важливі не тільки окремі рішення (закони, навчальні курси , програмно-технічні засоби захисту), що знаходяться на сучасному рівні, але і механізми генерації нових рішень, що дозволяють як мінімум адекватно реагувати на загрози інформаційної безпеки або передбачити нові загрози і вміти їм протистояти.

Нанесення шкоди власникові інформаційного ресурсу в цілому призводить до матеріальних витрат, а використання експертних систем може сприяти вирішенню цієї проблеми. Створення і використання експертних систем є одним з важливих етапів розвитку інформаційних технологій. Використання евристик дозволяє різко скорочувати кількість альтернативних варіантів при пошуку раціонального рішення неформалізованих задач.

Виявляється, що відносно нескладні евристики і знання багатьох експертів можуть бути представлені формально і реалізовані в рамках експертної системи. Тим самим експертні системи стають хорошим помічником фахівця в конкретній предметній області, особливо якщо кваліфікація фахівця не дуже висока. Експертні системи можна розглядати як своєрідні підсилювачі інтелектуальної творчої діяльності людини в даній предметній області, і в цьому полягає їх основне призначення. [3]

Переваги експертних систем в порівнянні з використанням досвіду фахівців полягають у наступному:

- досягнута компетентність не втрачається, може документуватися, передаватися, відтворюватися і нарощуватися;
- мають місце більш стійкі результати, відсутні емоційні та інші фактори людської ненадійності;
- висока вартість розробки врівноважується низькою вартістю експлуатації, можливістю копіювання, що в сукупності стає дешевшим за вартість висококваліфікованих фахівців.

Практична реалізація експертної системи полягає у прийнятті оптимального рішення з ефективного захисту інформаційних ресурсів організації. В даний час експертні системи можуть широко застосовуватися не тільки при проведенні аудиту безпеки інформаційних систем, але й індивідуально фахівцями на місцях для прийняття рішення щодо забезпечення безпеки інформаційних ресурсів організації. [2]

Недоліком експертних систем, характерним для їх сучасного стану, є менша пристосовність до навчання новим правилам і концепціям, до творчості і винахідництва. Використання ж експертних систем дозволяє в багатьох випадках відмовитися від висококваліфікованих фахівців, але завжди передбачає наявність експерта нижчої кваліфікації.

Таким чином, використовуючи експертні системи з базами знань за нормативними документами у сфері захисту інформації, з конкретними рішеннями по багатьом реальним можливим ситуаціям, можна значно спростити роботу фахівців і одночасно забезпечити їх самостійне навчання на даних прикладах, як на своєрідному тренажері.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Петренко Т.А. Інформаційна безпека в сучасних умовах. Вісник Чернігівського державного інституту права, соціальних технологій та праці (серія: Право. Економіка. Соціальна робота. Гуманітарні науки) [текст]: щоквартальний науковий збірник. – 2009. - №2. – Чернігів: ЧДІПСТіП, 2009.
2. Степанов В.Д. Система технісного захисту інформації в Україні: стан та напрями розвитку. – К., В збірнику наук. праць ""Захист інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності" ", вип.4(28), НАУ, 2009. – С.125-130.
3. Машкин М.Н. Информационные технологии: Учебное пособие. М.: ВГНА, 2008. –200 с.