УДК 519.86 + 338.5.018.7

Губка Д. О.,
Наук. керівник: Карпенко М. Ю.[1]

АУДИТ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Збільшення обсягу даних, що є конфіденційними з точки зору підприємств і обробляються в корпоративних інформаційних системах(ІС), веде не тільки до суттєвого збільшення капіталовкладень у ці інформаційні системи, але і робить залежною успішну діяльність цих підприємств від рівня захисту корпоративної інформації.

Особливо вразливими є корпоративні ІС, які використовують технології Internet/Intranet. Причинами такої ситуації є ускладнення програмних компонент, збільшення структурної та функціональної складності системного і програмного забезпечення, велика кількість користувачів тощо. Усі ці фактори ведуть до виникнення нових загроз у межах корпоративних ІС, промислового шпигунства внаслідок передачі інформації по відкритих каналах загального користування.

Тому сьогодні одним з найбільш актуальних напрямків стратегічного управління в області безпеки корпоративних систем є аудит інформаційної безпеки (ІБ) цих систем. Основним завданням такого аудиту є об'єктивна оцінка поточного стану ІБ, її адекватності поставленим цілям і перспективам економічної діяльності підприємств. В результаті якісно проведеного аудиту ІБ підприємств можна з мінімальними витратами побудувати ефективну корпоративну систему захисту.

Сьогодні на ринок технологій викидаються різні засоби забезпечення ІБ і підприємства прагнуть придбати найбільш ефективні і прийнятні з них. Але перед підприємствами виникають нові проблеми, пов'язані із сумісністю старих засобів забезпечення безпеки з новими підходами до захисту даних. Крім того виникає низка питань, як то: забезпечення цілісного управління різнорідними засобами безпеки; оцінка ризиків, які виникають внаслідок використання старого програмного забезпечення, рівень можливих втрат внаслідок руйнування системи захисту тощо.

Відповідь на всі ці питання дає аудит безпеки, який дозволяє оцінити поточну ІБ підприємств, прогнозувати і оцінювати ризики, забезпечити безпеку маркетингових програм, бухгалтерських та фінансових даних, баз даних підприємств в цілому. Позитивна практична сторона прояви аудиту ІБ полягає в тому, що він орієнтований не тільки на фахівців в області інформаційної безпеки корпоративних систем, а й на фахівців в області

[1] Губка Д. О, студент ХНУМГ ім. О. М. Бекетова,
Карпенко М. Ю., доцент кафедри Комп'ютерних наук та інформаційних технологій ХНУМГ ім. О. М. Бекетова,

менеджменту. Спільна робота таких фахівців у межах одного підприємства дозволить підвищити економічну ефективність діяльності цього підприємства, поліпшити його інформаційну безпеку.

Аудит інформаційної безпеки включає в себе кілька взаємопов'язаних етапів.

Перший етап – ініціювання процесу аудиту, коли керівник підприємства ставить питання і приймає рішення щодо проведення аудиту ІБ. На цьому етапі має бути обраний аудитор, який буде проводити аудит, обумовлені його права і обов'язки, складений план проведення аудиту, визначені межі проведення обстеження.

Другий етап має за мету збір інформації для подальшого аудиту. Цей процес може бути досить складним через відсутність необхідної документації на діючу ІС, він може бути пов'язаний з необхідністю взаємодії аудитора з великою кількістю співробітників підприємства. Спочатку аудитор збирає інформацію про організаційну структуру користувачів ІС, потім аналізує призначення і функціонування ІС та окремих її компонент. Наприкінці, маючи реальну інформацію про роботу системи, аудитор робить висновок щодо необхідності та напрямків подальшого аналізу зібраних даних.

На третьому етапі відбувається аналіз даних аудиту. Він проводиться, як правило, за двома напрямками, – аналіз ризиків, на основі якого вибирається індивідуальний набір вимог до безпеки, і аналіз відповідності стандартам ІБ, який визначає базовий набір вимог безпеки для більшості відомих ІС. Після чого починається розробка рекомендацій, які повинні бути конкретними, економічно обґрунтованими і адекватними до ІС підприємства.

Заключний етап – це складання звіту аудитора. У ньому викладаються цілі проведення аудиту, характеристика об'єкта дослідження (інформаційної системи), методи, використані при проведенні аудиту, результати аналізу, висновки.

Таким чином, для вироблення стратегії захисту комп'ютерної системи підприємства та здійснення ефективного управління ним необхідно задіяти аудит ІБ з метою визначення можливих вигід від впровадження нових технологічних і програмних засобів захисту даних.