

ДЕЯКІ ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМИ БЕЗПЕКИ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

Кузнєцов П. В., Сокол К. М.

Національний технічний університет

«Харківський політехнічний інститут», м. Харків

Серед напрямків електронної комерції, які активно розвиваються, важливу роль відіграють системи Інтернет-торгівлі Business to Consumer. Цей сектор бізнесу пов'язаний із наданням послуг або продукції кінцевому споживачеві. Основний тип даних систем – електронний магазин – автоматизована система електронної торгівлі в Інтернет. Вона являє собою характерний приклад розподіленої обчислювальної системи. Таким чином, електронному магазину загрожують усі внутрішні й зовнішні атаки, властиві будь-якій розподіленій комп'ютерній системі, взаємодіючої за допомогою передачі даних по відкритих мережах. Обоє учасника цього бізнес-процесу виявляються уразливими перед ними й незахищеними в плані відбиття атак, таких як: підміна сторінки Web-Сервера електронного магазину; проникнення в базу даних і зміна процедур обробки замовлень; реалізація атак типу «відмова в обслуговуванні» і порушення функціонування або виведення з ладу вузла електронної комерції; шахрайство з боку співробітників електронного магазину; перехоплення даних, переданих у системі електронної комерції й т. п.

Для вирішення проблем безпеки пропонуються наступні захисні заходи. На рівні мережі – застосування маршрутизаторів і міжмережєвих екранів, на рівні ж ОС – вбудованих засобів розподілення доступу. На рівні роботи з базами даних – застосування засобів аналізу захищеності й сканерів безпеки. Принципово новий підхід до здійснення електронних платежів сьогодні укладається в негайній авторизації й шифруванні фінансової інформації в Інтернет із використанням протоколів SSL (Secure Sockets Layer) і SET (Secure Electronic Transaction). Для захисту угод в Інтернеті в цей час організовані спеціальні центри сертифікації. Вони стежать за тим, щоб кожний учасник електронної комерції одержував унікальний електронний «сертифікат», у якому за допомогою ключа центра сертифікації підписано відкритий ключ даного учасника комерційних угод.

Таким чином, викладені вище вразливості необхідно вивчати й усувати. Від цього залежить обсяг продажу і, відповідно, прибутковість даного сектора електронної комерції. Спільне застосування різних засобів захисту на всіх рівнях дозволить побудувати надійну систему забезпечення інформаційної безпеки E-commerce.