

ЗАХИСТ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Губернаторов О.А.

Науковий керівник – к.т.н., доц. Войтович О.П.

Високий рівень шахрайств в Інтернеті є стримуючим чинником розвитку електронної комерції. Покупці бояться користуватися цією технологією через побоювання нести фінансові втрати. Ключовим питанням для впровадження даної технології є захист і безпека.

Найпоширенішими методами захисту в електронній комерції є стандарти Secure Sockets Layer (SSL) та Secure Electronic Transaction (SET). На даний момент 95% електронних транзакцій здійснюється з використанням стандарту SSL. Основними його перевагами є використання сертифікатів, шифрування даних, а також простота та дешевизна використання і впровадження. Недоліки – відсутність однозначної автентифікації користувача та Інтернет-магазину.

Всі недоліки SSL виправлено у стандарті SET. Перевагою даного протоколу є автентифікація користувача, магазину і банку, через який буде здійснюватись оплата, підтримка шифрування, сертифікація. Основним і, мабуть, найважливішим недоліком є ціна запровадження даної технології.

Вирішенням проблеми безпеки в електронній комерції є використання комплексних засобів захисту, які зможуть забезпечити автентифікацію користувачів (покупців та продавців), конфіденційність та цілісність даних при невеликих витратах. Одним з таких інструментів є досить відомий комплект протоколів IP Security (IPsec). Захист буде здійснено завдяки створенню політики безпеки IPsec, яка буде створювати захищений тунель між браузером клієнта та Інтернет-магазином.

Алгоритм створення тунелю.

1. Визначення типу трафіку і політики безпеки.
2. Автентифікація сторін і створення захищеного каналу, що дозволить почати обмін ключами IKE.
3. Вибір алгоритму шифрування, протоколу автентифікації (AH) та конфіденційності (ESP).
4. Створення захищеного тунелю.

Отже розглянуто основні методи та протоколи захисту. Виявлено переваги та недоліки кожного з методів і представлено альтернативний варіант побудови захисту. Планується більш детально вивчити запропоновану політику безпеки для забезпечення безпеки в електронній комерції.