

ЗАХИСТ ЕЛЕКТРОННИХ ПЛАТЕЖІВ НА ОСНОВІ ПРОТОКОЛУ IPSEC

Губернаторов О.А.

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

Сьогодні більш широкого застосування набуває міжбанківська система електронних платежів та взаєморозрахунків – комп'ютерна система електронного зв'язку, яка не може вважатися абсолютно надійною. Складається ситуація, що заохочує злочинців отримувати несанкціонований доступ до особистих даних клієнтів електронних магазинів.

Ключовим питанням для впровадження електронної комерції, зокрема в Україні, є забезпечення безпеки та захисту від шахрайств, тобто забезпечення цілісності, доступності, конфіденційності, автентичності даних та неможливості відмови від зобов'язань як покупців, так і самого електронного магазину.

Оскільки зміна базових протоколів сімейства TCP/IP викликала б повну перебудову мережі Інтернет, було поставлене завдання забезпечення безпеки інформаційного обміну у відкритих телекомунікаційних мережах на базі існуючих протоколів.

Найпоширенішими протоколами захисту в електронній комерції є використання стандартів Secure Sockets Layer (SSL) та Secure Electronic Transaction (SET). Основним недоліком протоколу SSL є відсутність однозначної автентифікації користувача та Інтернет-магазину. Недоліком протоколу SET є висока ціна запровадження цієї технології.

Розробки групи IPsec дозволяють організувати захищені тунелі між хостами, тунелі інкапсульованих даних і віртуальні приватні мережі, забезпечуючи таким чином захист протоколів, розташованих вище за рівень IP.

Основною метою роботи є побудова потужної системи захисту електронних платежів при невисоких затратах з боку кожного покупця, чого можна досягнути використовуючи стек протоколів IP Security (IPsec), який завдяки створенню політики безпеки IPsec, будує захищений тунель між браузером клієнта та сервером. Робоча група Інтернету (IETF) визначає IPsec як набір специфікацій для встановлення достовірності, цілісності та забезпечення конфіденційності засобами криптографії для протоколу IP.

Отже запропоновано використання протоколу IPsec для побудови захищеної системи електронних платежів. В подальшому планується розробити програмний засіб для реалізації запропонованого рішення.