Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації»

м. Вінниця, Україна
20-22 квітня 2011 року

Тезисы докладов Третьей Международной научно-практической конференции «Методы и средства кодирования, защиты и сжатия информации»

г. Винница, Украина
20-22 апреля 2011 года

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – 231 с.
ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

©Автори статей, 2011
©Упорядкування, Вінницький національний технічний університет, 2011

УДК 004.056

СИСТЕМА ЗАХИСТУ ЕЛЕКТРОННИХ ПЛАТЕЖІВ НА ОСНОВІ ПРОТОКОЛУ IPSEC

О. П. Войтович, к.т.н., доцент;
О. А Губернаторов, студент
Вінницький національний технічний університет
o_voytovych@mail.ru

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. Недолі-

ком протоколу SET є висока ціна запровадження цієї технології.

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.

IPsec призначався і фактично став стандартом для захисту Інтернет-комунікацій. 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.

Для побудови запропонованої системи необхідно:

1. Визначити загальний набір правил безпеки IPSec, які налаштовуються на мережевому обладнанні покупців та електронного магазину.
2. Підібрати набір правил для обробки мережевого трафіку, тобто визначити протокол автентицікації сторін.
3. Визначити набір фільтрів та дій, які будуть виконуватись над пакетами, тобто визначити алгоритми хешування та шифрування даних в TCP/IP мережах.
4. Автоматизувати процес побудови захисту, використовуючи програмний засіб або скрипт, в залежності від мережевого обладнання та операційної системи покупця.

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