ВИСНОВКИ

Криптологія як наука аналізує інформаційну безпеку. В роботі було реалізовано криптографічну систему обчислення ключів RSA. Наведено алгоритм та принцип шифрування даних.

ЛІТЕРАТУРА

1. Інформаційні Алфьоров А.П., Зубов А.Ю., Кузьмін А.С., Черьомушкін А.В. Основи криптографії: Навчальний посібник. 3-тє вид., 2005. - 480с.

Швець Дмитро Валерійович,
Карабут Надія Олександрівна
ст. викладачі
Криворізький національний університет

ЗАСОБИ ЗАХИСТУ ПЕРЕДАВАНОЇ ІНФОРМАЦІЇ В БЕЗДРОТОВИХ ЛОКАЛЬНИХ МЕРЕЖАХ

Проаналізовано застосування стеганографії в бездротових локальних мережах для забезпечення конфіденційності циркулюючої в ній інформації та контролю за доступом до пристроїв мережі.

Одним з методів забезпечення конфіденційності передаваної в мережі інформації є стеганографія. На відміну від криптографії, яка забезпечує шифрування повідомлення, що передається, стеганографія дає можливість надсилати інформацію таким чином, що при перехопленні пакетів залишається тайним питання наявності в цьому повідомленні зашифрованої інформації. Перевагою стеганографії над криптографією є те, що передаване повідомлення не викликає підозр щодо його вмісту за рахунок маскування факту наявності в ньому прихованих даних.

Методи, що забезпечують реалізацію передачі стеганограм в локальній бездротовій мережі, формують стеганографію WLAN. Прикладом, що реалізує стеганографію бездротових локальних мереж, є HICCUPS. Зазначена система передає кадри зі спотвореними контрольними сумами. Зазвичай, при передачі таких кадрів по локальній мережі відбувається їх відкидання терміналом. Але у випадку застосування відповідних програмних чи апаратних

засобів, що реалізують стеганографічні алгоритми, виконується аналіз відбракованих пакетів – замість їх ігнорування виконується сканування на предмет наявності у них стеганограм.

Використання спотворень та шумів зумовлює низьку вірогідність виявлення факту застосування цього методу. Для детектування використання HICCUPS потребується пошук засобів визначення кількості кадрів з некоректними контрольними сумами. Їх значна кількість може свідчити про наявність в них прихованих даних. Відповідно, детальний аналіз некоректних пакетів також може наблизити до виявлення в них прихованих даних.

ВИСНОВКИ

Таким чином, засоби стеганографії на кшталт HICCUPS реалізують зручний засіб прихованої передачі даних, що має переваги перед криптографією за рахунок приховування факту наявності в повідомленні прихованої інформації.

ЛІТЕРАТУРА

1. Szczypiorski, K.: HICCUPS: Hidden Communication System for Coruppted Networks. In Proc: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003. Międzyzdroje. 22-24 October 2004. pp.31-40