**АНОТАЦІЯ**

Кваліфікаційна робота 67 с., 22рис., 3 табл., 1 додаток, 13 джерел

Об’єкт розробки – дослідження часу підбору ключа шифрування RC4 в інформаційній мережі з тунельним доступом до неї через протокол PPTP.

Метою дослідження є підвищення безпеки та надійності доставки інформації в мережі шляхом збільшення розміру ключа шифрування RС4 у протоколі PPTP.

В ході розробки проведено:

* аналіз існуючих технологій VPN на базі брандмауерів, маршрутизаторів, програмного забезпечення, апаратного забезпечення, та на базі мережевої ОС;
* порівняння протоколів VPN, їх аналіз та вибір найбільш актуального для поставленої задачі;
* налаштування VPN з’єднання на базі Windows Server 2003;
* дослідження залежності часу підбору ключа шифрування RC4 у протоколі PPTP від його довжини.

**Ключові слова**: ДИСТАНЦІЙНО РОЗПОДІЛЕНА МЕРЕЖА, ТУНЕЛЮВАННЯ, ВІДДАЛЕНИЙ ДОСТУП, VPN, WINDOWS SERVER 2003, MITM, PPTP, RC4.

**АННОТАЦИЯ**

Квалификационная работа 67 с., 22 рис., 3 табл., 1 дополнение, 13 источников

Объект разработки – исследование времени подбора ключа шифрования RC4 в информационной сети с тунельным доступом к ней через протокол PPTP.

Целью исследования является повышение безопасности и надежности доставки информации в сети при помощи увеличения размера ключа шифрования RС4 в протоколе PPTP.

В ходе разработки проведено:

* анализ существующих технологий таких как VPN на базе брандмауэров, маршрутизаторов, программного обеспечения, аппаратного обеспечения, и на базе сетевой ОС;
* сравнение протоколов VPN, их анализ и выбор наиболее актуального для поставленной задачи;
* настрйка VPN соединения на Windows Server 2003;
* исследование зависимости времени подбора ключа шифрования RC4 в протоколе PPTP от его длины.

**Ключевые слова**: ДИСТАНЦИОННО РАСПРЕДЕЛЁННАЯ СЕТЬ, ТУННЕЛИРОВАНИЕ, УДАЛЁННЫЙ ДОСТУП, VPN, WINDOWS SERVER 2003, MITM, PPTP, RC4.

**Annotation**

Qualifying 67 p., 22 pic., 3 tables., 1 application, 13 sourses

The development object is a study of cracking time of RС4 encryption in PPTP.

The aim of the research is to increase the security and reliability of information delivery in the network by increasing the size of the RC4 encryption key in the PPTP protocol.

During the development was conducted:

* analysis of existing VPN technologies;
* comparison of VPN protocols and selection of the most relevant for the task;
* configuration VPN connection on Windows Server 2003;
* a study of the dependence of the cracking time of the RC4 encryption key to its length.

**Keywords:** REMOTE ACCESS NETWORK, VPN, TUNNELING, WINDOWS SERVER 2003, MITM, PPTP, RC4.