УДК 509.05.15.31
Пшиничняк О. – ст. гр. ПК-71
Тернопільський державний технічний університет імені Івана Пулюя

ЗАХИСТ ІНФОРМАЦІЇ В НЕЗАХИЩЕНИХ КАНАЛАХ ЗВ'ЯЗКУ

Науковий керівник: к.т.н., доц. Литвиненко Я. В.

В наш час інформаційні технології розвиваються надзвичайно швидкими темпами. Такий науковий розвиток призвів до того, що інформаційна безпека не тільки стає обов'язковою, вона також являється однією з характеристик інформаційних систем. Існує досить великий клас систем обробки інформації, при розробці яких фактор безпеки відіграє ключову роль (наприклад, банківські інформаційні системи тощо).

В наш час світ стурбований станом захисту національних інформаційних ресурсів у зв'язку з розширенням доступу до них через відкриті інформаційні мережі типу Internet. Крім того, збільшується число комп'ютерних злочинів, і тому реальною стала загроза інформаційних атак на більш високому рівні для досягнення політичних і економічних цілей.

До найбільш уразливих місць, через які зазвичай намагаються проникнути зловмисники, належать відкриті системи, системи, що підтримують технологію підключення периферійних пристроїв у режимі plug-and-play, засоби централізованої віддаленої підтримки, канали комутації віддаленого доступу та недостатньо надійні технології шифрування. В даній доповіді будуть розглянуті методи захисту інформації в незахищених каналах зв'язку.

На сьогодні для забезпечення захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, який включає комплекс взаємозалежних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії, тощо). Комплексний характер захисту випливає з комплексних дій зловмисників, які прагнуть будь-якими способами добути важливу для них інформацію.

Серед розглянутих методів захисту інформації в доповіді зроблений акцент на використанні відомого алгоритму кодування інформації Blowfish. До його переваг перед іншими належать:

- Швидкість. Blowfish шифрує дані на 32-бітових мікропроцесорах із швидкістю 26 тактів на байт.
- Компактність. Blowfish може працювати менш, ніж в 5 Кбайт пам'яті.
- Простота. Blowfish використовує тільки прості операції: додавання, XOR і вибірка з таблиці по 32-бітовому операнду. Аналіз його схеми нескладний, що дає можливість при реалізації алгоритму зменшити кількість помилок .
- Налаштування ступеня безпеки. Довжина ключа Blowfish перемінна й може досягати 448 біт.