УДК 004.421.5

Боєчко І. – ст. гр. ПКзпм-61, Бідзюра Р. – ст. гр. ПКзпм-61, Мазурок Ю. – ст. гр. ПКмп-61

Тернопільський державний технічний університет імені Івана Пулюя

РОЗРОБКА ІМОВІРНІСНОЇ МОДЕЛІ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Науковий керівник: асистент Шимчук Г.В.

Стрімкий розвиток засобів обчислювальної техніки і відкритих мереж, сучасні методи накопичення, обробки і передачі інформації сприяли появі погроз, пов'язаних з можливістю втрати, розкриття, модифікації даних, що належать кінцевим користувачам.

Основу забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах складають криптографічні методи і засоби захисту інформації.

В зв’язку з цим була поставлена задача провести системний аналіз роботи криптографічних протоколів і створити математичні імовірнісні моделі елементів криптографічних систем і самих протоколів з метою формалізації оцінок стійкості криптопротоколів.

Для досягнення мети було вирішено наступні завдання.

1. Було проаналізовано структуру захищених систем, що використовують криптографічні протоколи. В загальному вигляді її можна описати так.

2. Проаналізував методики оцінки стійкості криптографічних шифрів і протоколів.

3. Розробив пропозицій по формалізації завдання оцінки стійкості протоколів, заснованої на імовірнісних моделях, привів приклад аналізу стійкості протоколу з нульовим розголошенням на основі його імовірнісної моделі.

Криптосистема, що аналізується повинна обиратися і розроблятися досить ретельно. Аналіз повинен показати, що обрана система відповідає висунутим вимогам, які також повинні бути строго формалізовані.

Формальні методи системного аналізу використовують систематичні процедури, строгість яких забезпечується математичними засобами. Ці процедури дозволяють або розробляти системи, що володіють наперед заданими властивостями, або перевіряти вже існуючі системи, щоб виявити можливі приховані помилки.

Література:

1. Добрынин В. Ю., Некрестьянов И. С. “Задача выбора тематических коллекций, релевантных запросу”. Труды Всероссийской научно-методической конференции "Интернет и современное сообщество", Санкт-Петербург, декабрь 1998.
2. Лунегов С. В., Некрестьянов И. С. «Нормализация документов для полнотекстового поиска». Труды Всероссийской научно-методической конференции "Интернет и современное сообщество", Санкт-Петербург, декабрь 1998.