

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАТИКА, МАТЕМАТИКА,
АВТОМАТИКА

ІМА :: 2017

**МАТЕРІАЛИ
та програма**

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 17–21 квітня 2017 року)



Суми
Сумський державний університет
2017

Розробка схеми оцінювання ефективності впровадження нових криптографічних алгоритмів захисту трафіку в телекомунікаційній мережі

Єременко О. С., докторант, Персіков А. В., здобувач
Харківський національний університет радіоелектроніки,
м. Харків

Сучасні телекомунікаційні мережі (ТКМ) є розподіленими системами, що забезпечують взаємодію множини пов'язаних об'єктів за допомогою універсальної транспортної мережі, здатної передавати різнотипні дані з необхідними параметрами якості обслуговування відповідно до угоди про якість обслуговування. Однією з базових задач, яка регламентується стандартами побудови ТКМ, є завдання реалізації функцій інформаційної безпеки.

Були проаналізовані різні технології організації криптографічно захищеного каналу, розглянуті протоколи проведення аутентифікації об'єктів телекомунікаційної мережі, виділені загальні риси та відмінності при обробці стеками протоколів множини видів трафіку, що передається в транспортній мережі ТКМ. Проведений аналіз виявив необхідність перегляду відповідних протоколів з метою розділення інформаційних потоків, що дозволить протоколам бути схваленими для реалізації в мережах, де циркулює інформація з обмеженим доступом, і збільшити швидкість системи обробки інформації за рахунок одночасного проведення операцій над множиною потоків даних.

У зв'язку з цим була запропонована схема оцінювання ефективності впровадження нових методів криптографічного захисту в рамках існуючих і розроблюваних протоколів обміну даними з урахуванням вимог, визначених угодою про якість обслуговування інформаційних потоків. Така схема може бути використана при тестуванні відповідності криптографічних алгоритмів, модулів і захищених протоколів обміну даними й управління ключами в ході інформаційного обміну в телекомунікаційній мережі.