УДК 658.012.011.56:681.3.06

М. Карпінський[1], Я. Кінах[1], У. Яциковська[2], І. Якименко[2], М. Касянчук[2]
([1]Тернопільський національний технічний університет імені Івана Пулюя)
([2]Тернопільський національний економічний університет)

УДОСКОНАЛЕННЯ АРХІТЕКТУРИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ КРИПТОАНАЛІТИЧНИХ АЛГОРИТМІВ

З метою уникнення непродуктивних операцій архітектуру мережі для криптоаналізу необхідно доповнити системним блоком, який реалізує правила оптимізації. В результаті отримаємо оптимізовану архітектуру криптоаналітичної мережі. Особливістю даної архітектури, яка характеризується оптимізованими програмами для серверів та робочих станцій є виключення взаємообернених функцій, які збільшують кількість операцій крипто аналітичного алгоритму та призводять до суттєвого зростання часу крипто аналізу[1]. На вхід подається програма, у виді композиції типових алгоритмічних структур ТАС. Транслятор, використовуючи шаблони – заготовки, розроблені з розрахунку на абстрактну робочу станцію, перекладає вихідну програму на проміжне представлення. Далі виконується фаза оптимізації інтерфейсу між ТАС криптоалгоритму. Математичну суть цього процесу детально розглянуто [2]. На останній фазі виконується переклад оптимізованої програми в кінцеву програму за допомогою штатного транслятора, що використовується системою [3]. Отримані за допомогою вищезгаданих механізмів оптимізації програми, мають спільну рису. В ієрархічному представлені глобальна структура програми крипто аналітичного алгоритму та всі її не термінальні вершини відповідають одиничним ТАС, оскільки всі вони, за винятком послідовних, мають єдину регулярну структуру, що подана деякою ТАС. Проміжне представлення не залежить від типу системи. Спеціалізація на конкретну архітектуру здійснюється на фазі оптимізації заданням параметрів. В процесі оптимізації використовуються параметричні оцінки ефективності ТАС. Ці оцінки, як і програмний код, не залежать від типу системи, оскільки аналітичний вираз криптоалгоритму інваріантний до конкретної обчислювальної системи [4]. Настроювання на систему здійснюється через параметри абстрактної робочої станції, що визначаються для кожного комп'ютера шляхом програмного тестування.

Дослідження показали, що передача даних по каналах зв'язку займає 9% часу розв'язку поставленої задачі, час роботи серверів – 12%, а робочих станцій – 79%. Відповідно до проведених дослідів час криптоаналізу на робочих станціях зменшиться на 12%, порівняно з традиційним мережним криптоаналізом.

Література

1. Горбенко И.Д., Горбенко Ю.И. Прикладная Криптология. – Харьков. Форт. – 2012, – С. 867.
2. Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів / Наукоємні технології. – 2013. – No3 (19) / Технічні науки. – С. 299 – 304.
3. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К.: НАУ, 2011. – 640 с.
4. Корченко О., Петров О., Лахно В. Метод та модель інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспорту. / Безпека інформації –2015 – No 1, Том 21. – с. 26 – 34.