УДК 004.087.5
Висоцький В.Я. – ст. гр. СІм-51
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ SMART-CARD

Науковий керівник: к.т.н., доцент Луцків А.М.

Смарт-картка (smart-card – інтелектуальна картка) – це пластиковий прямокутник, аналогічний за розмірами до карток з магнітною смугою. Замість смуги (чи додатково до неї) в таку картку вбудований мікропроцесор (як правило, 8-розрядний), пам'ять постійного типу для збереження операційної системи та прикладних програм і пам'ять для збереження змінних даних, що може перепрограмовуватися.

Крім того, до електросхеми включені й компоненти, що забезпечують виконання вводу-виводу даних, захист інформації, яка зберігається та спеціалізовані співпроцесори для прискореного виконання криптографічних операцій. Таким чином, вбудована в картку мікросхема є спеціалізованою мікроЕОМ, можливості якої забезпечують високий ступінь захисту від підробки і яка підтримує файлову організацію збереження даних та необхідний набір операцій з обробки інформації.

Проблемою захисту інформації шляхом її перетворення займається криптологія (kryptos - таємний, logos - повідомлення). Вона має два напрямки: криптографію і криптоаналіз. Цілі цих двох напрямків прямо протилежні. Криптографія займається пошуком, дослідженням і розробкою математичних методів перетворення інформації, основою яких є шифрування, а криптоаналіз - дослідженням можливості розшифровки інформації.

Останнім часом спостерігається тенденція по розширенню сфер застосування смарт-карт, що обумовлюється їх ціновою доступністю, а водночас високою ненадійністю та необхідністю заміни широко поширених пластикових карт з магнітним збереження даних. Тому варто очікувати суттєвого збільшення сфер застосування й кількості інформаційних систем з аутентифікацією на основі смарт-карт. Водночас до основних недоліків сучасних смарт-карт належать:

- недостатня апробація криптографічних засобів захисту, які в них використовуються, що дозволяє зловмиснику відносно просто отримати інформацію, яка на них зберігається;
- ненадійна схемотехнічна організація відповідних смарт-карт — зловмисник може отримати приховану інформацію на основі так званих побічних атак (англ. "side attacks"): візуальним, електричним та іншими методами;
- зосередженість виробництва смарт-карт у єдиних виробників, яких, на сьогодні, є відносно небагато, а відповідно використовувані в них технології не мають суттєвих відмінностей; це дає змогу суттєво спрощувати атаки зловмисників.

Оскільки, вплинути на технологічний процес виробництва смарт-карт є відносно складно, тому з метою усунення цих недоліків необхідно здійснювати детальну апробацію криптографічних методів захисту. А саме, розробляти програмне забезпечення з використанням надійних криптографічних бібліотек й враховувати основні розробки фахівців у галузі інформаційної безпеки.