

УДК 343.9

Владислав Сергійович ШЕСТОПАЛЮК,

курсант групи Ф4-201 ХНУВС

Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ЗАСТОСУВАННЯ ПРИКЛАДНОЇ КРИПТОГРАФІЇ, ЇЇ ВИДИ ТА МЕТОДИ

На сьогодні в інформаційному просторі, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Внаслідок цього різко зріс інтерес широкого кола користувачів до проблем захисту інформації. В останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу (НСД) до конфіденційної інформації. Серед всього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи.

Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Види дій над інформацією:

1. Блокування інформації (користувач не може дістати доступ до інформації; за відсутності доступу сама інформація не втрачається).

2. Порушення цілісності (втрата, вихід з ладу носія; порушення смислової значущості; порушення логічної зв'язаності; втрата достовірності).

3. Порушення конфіденційності (з інформацією ознайомлюються суб'єкти, на яких це не покладено). Рівень допуску до інформації визначає її власник. Порушення конфіденційності може відбутися із-за неправильної роботи системи обмеження доступу або наявності побічного каналу доступу.

Симетричне шифрування є запобігання перехоплення даних третіми особами і базування на тому, що відправник і одержувач даних не має однакові ключі для розгадки шифру.

Асиметричне шифрування – це задіяння відкритих і секретних ключів. Ці ключі взаємопов'язані інформацією, зашифровані відкритим ключем, які можуть бути розкриті тільки зв'язаним з ним секретним ключем. Застосувати для розгадки ключі різних пар не можливо, оскільки вони пов'язані між собою математичною залежністю.

Якщо розглянути хешування, то всі хеш-коди мають унікальну послідовність символів. Електронний підпис в своєму роді поєднаний з асиметричним шифруванням в тому плані, що він перетворює інформацію з використанням закритого ключа, що дозволяє підтвердити справжність документа і відсутність спотворення даних.

Серед всього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи, також хотів би відмітити, що на мою думку криптографічні методи застосовуються для:

- безпечного зберігання інформації комерційними і приватними особами;
- реалізації систем цифрового електронного підпису;
- підтвердження достовірності сертифікатів;
- захисту передачі даних онлайн по відкритих каналах зв'язку.

Криптографія є важливою складовою сучасного світу і необхідна в першу чергу для збереження персональних даних та іншої важливої інформації. Сучасні методи криптографії застосовуються практично у всіх галузях, в яких присутня необхідність безпечної передачі або зберігання даних.

Одержано 13.04.2019



**НАУКОВИЙ ГУРТОК
КАФЕДРИ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ
ТА РОЗКРИТТЯ ЗЛОЧИНІВ ФАКУЛЬТЕТУ № 2**

УДК 343.13

Віталій Олегович НАЙДА,
курсант групи Ф1-303 ХНУВС

Науковий керівник: кандидат юридичних наук, доцент Грабазій І. А.

**ОКРЕМІ ПИТАННЯ ВЗАЄМОДІЇ ОПЕРАТИВНИХ
ПІДРОЗДІЛІВ І НАСЕЛЕННЯ**

Реформи у правоохоронній сфері України покликані збільшити рівень довіри громадян до державних органів загалом та до Національної поліції зокрема, а також перевести довіру населення в практичну площину, тобто сформувати на її основі взаємодію.

У світлі зазначених реформ оперативні підрозділи Національної поліції переживають період якісних трансформацій, який полягає у докорінному переосмисленні питання взаємодії з населенням, формуванні у цьому аспекті нового бачення взаємодії поліції з громадою, за яким остання виступає повноцінним партнером поліції у протидії криміналітету.

Відповідно до Академічного тлумачного словника української мови під взаємодією в широкому значенні цього слова розуміють взаємний зв'язок між предметами у дії, а також погоджена дія між ким-, чим-небудь.

В свою чергу у ч. 1 ст. 11 Закону України «Про Національну поліцію» закріплене положення, що діяльність поліції здійснюється в тісній співпраці та взаємодії з населенням, територіальними громадами та громадськими об'єднаннями на засадах партнерства і спрямована на задоволення їхніх потреб.

Взаємодія оперативних підрозділів поліції і населення сьогодні повинна бути добровільною, неформальною і служити, насамперед, інтересам громадян.