УДК 004.021(043.2)

СПОСІБ ПОЄДНАННЯ ЗАВАДОСТІЙКОГО КОДУВАННЯ ТА ПОТОКОВОГО ШИФРУВАННЯ

Дубров О.
науковий керівник – к.т.н., доцент Семеренко В.П.

В багатьох телекомунікаційних системах використовуються шифрування для забезпечення безпеки інформації та різні види кодування, що перетворює інформацію у зручний для передачі вигляд. Метою розробки даного способу є поєднання шифрування і кодування у часі. Для досягнення цієї мети запропонований спосіб має володіти достатньою швидкодією, простотою реалізації, надійністю і гнучкістю.

На відміну від кодування, шифрування повинне реалізовувати найзаплутаніший зв'язок вхідної послідовності із зашифрованою. Тому у шифруванні активно використовуються нелінійні перетворення.

Запропонований спосіб використовує несистематичне кодування циклічних кодів, які реалізують першу «лінію» захисту. Це є наслідком того, що у такого виду коду неможливо визначити позиції перевірочних і інформаційних розрядів.

$$C(x) = I(x) \times g_1(x)$$

Другим ступенем захисту інформації є використання різного сеансового ключа K_{si} для кожного закодованого вектора. Задамо базовий сеансовий ключ, а також виберемо незвідний примітивний твірний поліном. Поточний сеансовий ключ буде обчислюватися як остача від ділення базового ключа на вибраний поліном:

$$K_{si} = K_b \ mod \ g_2(x)$$

Далі проведемо конкатенацію сеансового ключа та кодового вектора, і знаходимо зашифрований кодовий вектор, як остача від діленням $K_s||C(x)$ на твірний поліном, що використовувався для обчислення сеансового ключа. Таким чином отримуємо закодований і зашифрований кодовий вектор, готовий для передачі в канал зв’язку:

$$C_ш(x) = (K_s||C(x)) \ mod \ g_2(x)$$

Для розшифрування приймальна сторона має сформувати поточний сеансовий ключ K_s, аналогічно, як і на передавальній стороні. Далі приймальна сторона розшифровує кодовий вектор таким чином:

$$C(x) = C_ш(x) + K_s$$

Декодування проходить відомим способом – діленням кодового вектора $C(x)$ на твірний поліном кодування $g_1(x)$, та перевіркою остачі.

В запропонованій системі захисту базовий сеансовий ключ є таємним і однаковим для обох сторін, і тому такий шифр належить до симетричних шифрів.