46-та наукова конференція молодих дослідників ОНПУ-магістрантів
"Сучасні інформаційні технології та телекомунікаційні мережі". Одеса: ОНПУ, 2011, вип. 46.

ПРОБЛЕМИ СПІЛЬНОГО ВИКОРИСТАННЯ КОДУВАННЯ І ШИФРУВАННЯ

Стеценко А.О.

Науковий керівник – зав. каф. «Інформаційної безпеки»

док. техн. наук, проф. Мазурков М.І.

Коди контролю помилок використовуються в цифровому зв'язку чи для виявлення чи для виправлення помилок передачі. Такі коди зазвичай дуже відомі та не забезпечують криптографічного захисту.

Коли криптографічне кодування та кодування з ціллю контролю помилок використовується разом, то будь-яка операція може виконуватись першою, однак це призводить до різних результатів.

Якщо першим виконується кодування для контролю помилок, то у точці прийому першим виконається дешифрування. У випадку блочних шифрів цей метод має переваги, так як забезпечує високий рівень захисту за рахунок того, що супротивник не в змозі породити криптограму, котра після дешифрування буде мати необхідні значення в бітах контролю помилок. Якщо замість цього зовнішнім є код контролю помилок, то супротивник в змозі вводити помилкові повідомлення, які пройдуть крізь пристрій захисту від помилок. Тому імітостійкість вимагає внутрішнього механізму захисту від помилок.

Деякі розмірковування показують, що розмноження помилок при дешифруванні, що не дозволяє виправляти помилки за допомогою внутрішнього коду з контролем помилок, є необхідним для забезпечення імітостійкості. Синхронний потоковій шифр не призводить до розмноження помилок і за цих умов не забезпечує імітостійкості при його

використанні з фіксованим лінійним кодом контролю помилок, оскільки супротивник знає, які біти контролю помилок треба змінити при зміні бітів у повідомленні. І навпаки, виправлення помилок у випадку синхронного потокового шифру можливо реалізувати і внутрішньо, і зовнішньо.

Але якщо мислити раціонально, та піти по інтенсивному шляху розвитку, то висновок напрошується сам собою, - необхідно лише об'єднати ці дві операції в одному блоці. У наш час існує алгоритм який цілком в змозі реалізувати цю ідею. За основу алгоритму взято Досконалі Двійкові Решітки та їх властивості. Алгоритм здійснює шифрування повідомлення в реальному часі, а потім дешифрування на другому боці, також у реальному часі, при цьому об'єднуючи шифрування та завадостійке кодування в одному блоці. Якщо алгоритм зарекомендує себе в реальних умовах. То є велика вірогідність, що згодом від замінить систему з двох блоків кодування та шифрування, тому, що він позбавлений проблеми вибору розміщення цих блоків один після одного, а отже об'єднує тільки позитивні риси їх взаємного розташування.