МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ГРИШАКОВ Сергій Володимирович

УДК 003.26:004.056.55

МЕТОД ПОБУДОВИ РАНДОМІЗОВАНИХ ПОТОКОВИХ ШИФРОСИСТЕМ З НЕЛІНІЙНИМ ВИПАДКОВИМ КОДУВАННЯМ

21.05.01 – «Інформаційна безпека держави»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ 2018

Дисертацією є рукопис.

Робота виконана в Інституті спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ.

Науковий керівник: доктор технічних наук, доцент
Олексійчук Антон Миколайович,
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
головний науковий співробітник науково-дослідного центру.

Офіційні опоненти: доктор технічних наук, професор
Кузнецов Олександр Олександрович,
Харківський національний університет імені В.Н. Каразіна,
професор кафедри безпеки інформаційних систем і технологій;

кандидат технічних наук
Кінзерявий Василь Миколайович,
Національний авіаційний університет,
доцент кафедри безпеки інформаційних технологій.

Захист відбудеться «27» вересня 2018 р. о $15^{\underline{00}}$ годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, просп. Космонавта Комарова, 1, ауд. 11-111.

З дисертацією можна ознайомитись у бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, просп. Космонавта Комарова, 1.

Автореферат розісланий «27» серпня 2018 р.

Учений секретар спеціалізованої
вченої ради Д 26.062.17
д.т.н., доцент С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. З огляду на зростання рівня зовнішніх загроз національній безпеці та суверенітету України, особливої гостроти набувають задачі забезпечення інформаційної безпеки держави. Одним із основних напрямків вирішення цих задач є створення нових та удосконалення існуючих методів криптографічного захисту інформації, спрямованих на забезпечення конфіденційності, цілісності, справжності та доступності інформації.

На сьогодні криптографічні системи є невід'ємним елементом спеціальних інформаційно-телекомунікаційних систем (СІТС). Реалізації криптосистем повинні бути швидкими (здатними функціонувати в режимі реального часу на різних програмних і апаратних платформах) та криптографічно стійкими до всіх відомих криптоаналітичних атак. Особливо це стосується спеціальних (військових) додатків, витоки конфіденційної інформації в яких створюють ризики для інформаційної безпеки держави. Такими додатками є ті, в яких: часто трапляються випадки компрометації шифрувальної апаратури або алгоритму шифрування, відмови системи блокування шифратора, внаслідок чого в канал передачі може потрапити «слабка» гама шифрування; передаються короткі повідомлення (спеціальні команди чи військові накази); є невеликим навантаження на інформаційний трафік; криптографічна стійкість є важливішою за швидкість передачі інформації; є невеликою кількість абонентів; алгоритм шифрування може бути невідомим.

Широку розповсюдженість для захисту інформації в СІТС отримали потокові шифри, які представляють собою шифри з секретним ключем, де кожний символ відкритого тексту перетворюється в символ шифрованого в залежності не тільки від ключа, що використовується, але і від розташування символу у відкритому тексті. Звичайно такі шифри складаються з лінійних регістрів зсуву та компонент, що реалізують нелінійні перетворення. Основною перевагою потокових шифрів над блоковими є значно вища швидкість шифрування, зокрема, програмні реалізації слово-орієнтованих потокових шифрів є в 5 – 10 разів швидшими у порівнянні з відповідними реалізаціями блокових шифрів. Крім того, потокові шифри є більш придатними для застосування у пристроях з обмеженими обчислювальними ресурсами або з малим споживанням електроенергії.

Відомо, що стійкість будь-якого сучасного шифру залежить від розвитку методів криптоаналізу та можливостей криптоаналітика і має тенденцію зменшуватися з часом. Особливо це стосується потокових шифрів, різноманіття конструкцій яких (в порівнянні з блоковими) надає криптоаналітику більше потенційних можливостей для створення нових методів криптоаналізу та побудови нових атак, зокрема, таких, що можуть бути реалізовані на практиці. Характерним прикладом є алгоритми шифрування A5/1 та A5/2, які були

зламані одразу ж після оприлюднення їх описів.

Таким чином, неухильний розвиток інформаційних технологій поряд з нарощуванням потужності обчислювальних засобів та появою нових (або підсиленням відомих) методів криптоаналізу створює потенційну загрозу для СІТС, де використовуються потокові шифри. Оскільки швидка заміна алгоритму шифрування, криптографічні слабкості якого виявлені на етапі його експлуатації (як правило, через багато років після його створення) є практично неможливою (або організаційно та коштовно затратною справою), видається доцільним створення методів підвищення стійкості потокових шифрів без внесення змін в алгоритми шифрування шляхом застосування додаткових перетворень, які не потребують ключів, можуть бути відносно просто реалізовані та забезпечують науково обґрунтований рівень стійкості систем шифрування в цілому.

Одним з таких загальних методів є так звана рандомізація або випадкове кодування джерела відкритих повідомлень. Зауважимо, що метод рандомізації є відомим достатньо давно, проте (саме для випадку потокових шифрів) його можливості досліджені не повністю. Імовірно, єдиним відомим прикладом рандомізованих потокових шифросистем (РПШ), які будуються на регулярній основі та, в принципі, можуть бути використані на практиці, є шифросистеми Міхалевича-Імаї. Рандомізатори зазначених РПШ будуються на основі двійкових лінійних перетворень, зокрема, завадостійкого кодування відкритих повідомлень лінійними кодами. Проте стійкість РПШ Міхалевича-Імаї суттєво залежить від будови їх компонент і може бути значно менше, ніж стверджують їх розробники. Деякі з цих шифросистем виявляються вразливими навіть до атак на основі відомих шифрованих повідомлень і, отже, не можуть бути використані для захисту державних інформаційних ресурсів. Наведені факти свідчать про актуальність *наукової задачі розробки методу побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням для забезпечення безпеки державних інформаційних ресурсів*, розв'язанню якої присвячено дану дисертаційну роботу.

Зв'язок роботи з науковими програмами, планами, темами. Робота над дисертацією проводилася в рамках науково-дослідної роботи "Кета" (номер держреєстрації 0114U004643) на замовлення Служби зовнішньої розвідки України та відповідно до планів науково-дослідної роботи Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Мета та задачі досліджень. Метою дисертаційної роботи є підвищення криптографічної стійкості потокових шифрів шляхом рандомізації джерела відкритих повідомлень для забезпечення безпеки державних інформаційних ресурсів.

Для досягнення поставленої мети **необхідно розв'язати такі основні задачі:**

1. Провести аналіз відомих методів побудови рандомізованих шифросистем для забезпечення безпеки державних інформаційних ресурсів.

2. Отримати аналітичні оцінки обчислювальної стійкості РПШ Міхалевича-Імаї відносно атак на основі відомих шифрованих повідомлень, а також підібраних векторів ініціалізації.

3. Довести, що клас РПШ Міхалевича-Імаї (незалежно від будови їх компонент) володіє суттєвою слабкістю, яка полягає в зменшенні кількості інформації (в порівнянні з довжиною блоку шифрувальної гами), що необхідна для відновлення за реальний час символів відкритого тексту.

4. Отримати аналітичні межі для швидкості передачі інформації в РПШ Міхалевича-Імаї при заданих обмеженнях відносно стійкості та ймовірності правильного прийому повідомлень законним користувачем.

5. Розробити метод побудови РПШ з нелінійним випадковим кодуванням та отримати аналітичні оцінки обчислювальної стійкості цих шифросистем відносно відомих атак; встановити та обґрунтувати вимоги до нелінійних відображень в конструкціях рандомізаторів РПШ з нелінійним випадковим кодуванням, що визначають стійкість цих РПШ відносно зазначених атак.

6. Провести порівняння РПШ Міхалевича-Імаї і РПШ з нелінійним випадковим кодуванням за швидкістю передачі (при фіксованій стійкості) та стійкістю шифрування (при фіксованій швидкості передачі); розробити програмні реалізації запропонованих РПШ на базі нелінійних відображень і гешфункцій та виконати порівняння ефективності цих програмних реалізацій.

Об'єктом дослідження в дисертаційній роботі є процес криптографічного перетворення інформації у рандомізованих потокових шифросистемах, а *предметом дослідження* – методи побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням, призначених для забезпечення безпеки державних інформаційних ресурсів.

Методи дослідження. Основу дисертаційних досліджень складають теоретичні дослідження (математичні методи оцінювання обчислювальної стійкості рандомізованих потокових шифросистем). Для аналізу існуючих методів побудови рандомізованих шифросистем, а також розробки методу побудови РПШ з нелінійним випадковим кодуванням застосовувались методи лінійної алгебри, теорії ймовірностей та теорії інформації. Дослідження стійкості РПШ Міхалевича-Імаї та РПШ з нелінійним випадковим кодуванням здійснювалось з використанням методів лінійної алгебри, теорії ймовірностей, математичної статистики, а також теорії складності обчислень. При побудові аналітичних меж для швидкості передачі інформації в РПШ Міхалевича-Імаї застосовувались методи теорії кодування. Чисельні розрахунки на обчислювальній системі та розробка програмних реалізацій РПШ з нелі-

нійним випадковим кодуванням виконувалися з використанням середовища розробки Microsoft Visual Studio 2013 (компонент Visual C++).

Наукова новизна одержаних результатів. Підсумком розв'язання зазначених наукових задач є такі нові наукові результати, що висуваються на захист:

1. *Вперше* отримано аналітичні оцінки параметрів, що визначають стійкість РПШ Міхалевича-Імаї відносно атак на основі відомих шифрованих повідомлень, а також підібраних векторів ініціалізації. Отримані оцінки *дозволяють* з'ясувати теоретико-кодовий сенс параметрів, які визначають обчислювальну стійкість цих шифросистем, а також встановити, що їх стійкість може бути значно менше, ніж стверджують їх розробники, що досягається *за рахунок* розширення можливостей супротивника при проведенні зазначених атак.

2. *Вперше* доведено, що клас РПШ Міхалевича-Імаї (незалежно від будови їх компонент) володіє суттєвою слабкістю, яка полягає в зменшенні кількості інформації (в порівнянні з довжиною блоку шифрувальної гами), що необхідна для відновлення за реальний час символів відкритого тексту. Зазначена властивість *дозволяє* зробити практично важливий висновок про те, що для відновлення символів відкритого тексту супротивнику достатньо мати лише часткову інформацію про секретний ключ РПШ, що відбувається *за рахунок* спільного застосування випадкового і завадостійкого кодування повідомлень лінійними кодами.

3. *Вперше* отримано аналітичні межі для швидкості передачі інформації в РПШ Міхалевича-Імаї при заданих обмеженнях щодо ймовірності правильного прийому повідомлень законним користувачем та стійкості шифрування. Зазначені межі, *за рахунок* застосування оцінок Плоткіна та Бассалиго-Елайєса для швидкості передачі лінійних кодів, *дозволяють* зробити науково обґрунтований висновок про обмежені можливості РПШ Міхалевича-Імаї з погляду сучасних вимог щодо стійкості та практичності в реальних умовах.

4. *Отримав подальший розвиток* метод побудови РПШ, який, *на відміну від раніше відомих*, базується на застосуванні для випадкового кодування нелінійних відображень або безключових геш-функцій та *дозволяє* збільшити стійкість в порівнянні з РПШ Міхалевича-Імаї *за рахунок* розширення класу перетворень, які використовуються в конструкції рандомізатора.

Практичне значення одержаних результатів. Розроблено програмні реалізації РПШ з нелінійним випадковим кодуванням на основі нелінійних відображень та безключових геш-функцій, що є більш стійкими (у 2^{242} і більше разів) і більш швидкісними (у 125 і більше разів) в порівнянні з раніше відомими РПШ при однаковій довжині вихідного повідомлення. Розроблені реалізації РПШ дозволяють здійснювати процедури зашифровування/роз-

шифровування даних в режимі реального часу та можуть бути використані на практиці у спеціальних (військових) додатках, витоки конфіденційної інформації в яких створюють ризики для інформаційної безпеки держави.

Наукові та практичні *результати дисертаційної роботи реалізовані* в Службі зовнішньої розвідки України – в результаті виконання НДР «Кета» (акт від 14.09.2016) та в науково-технічних розробках ЗАО «Інститут інформаційних технологій» (акт від 25.07.2016).

Особистий внесок здобувача. У [1, 9] автором отримано неасимптотичні оцінки ймовірності правильного відновлення символу відкритого тексту за символом шифротексту РПШ з нелінійним випадковим кодуванням; в [2, 10] автору належать ефективні алгоритми нелінійного випадкового кодування і декодування повідомлень; в [3, 11, 12] автором отримано аналітичні оцінки ймовірності правильного прийому відкритих повідомлень в системах передачі інформації з випадковим кодуванням; в [4] автором запропоновано атаку на РПШ Міхалевича-Імаї на основі відомих шифрованих повідомлень, а також атаку на основі підібраних векторів ініціалізації, для якої отримано верхні оцінки обчислювальної складності; в [5] автором отримано верхні оцінки обчислювальної складності атаки на РПШ з нелінійним випадковим кодуванням на основі підібраних векторів ініціалізації; в [6, 13] автором запропоновано метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням та отримано верхні оцінки обчислювальної складності атак на такі шифросистеми; в [7] автором отримано верхні оцінки швидкості передачі інформації в РПШ Міхалевича-Імаї при заданих обмеженнях відносно ймовірності правильного прийому повідомлень законним одержувачем і стійкості шифрування; крім того, встановлено нижню межу для максимальної швидкості передачі інформації, при якій існують РПШ Міхалевича-Імаї із заданою стійкістю; в [8, 14, 15] автору належить неасимптотична нижня межа складності атаки на РПШ Міхалевича-Імаї на основі підібраних векторів ініціалізації.

Апробація результатів дисертації. Результати дисертаційних досліджень доповідалися та обговорювалися *на 7 міжнародних наукових конференціях*: VII – XVII Міжнародних науково-практичних конференціях «Безпека інформації в інформаційно-телекомунікаційних системах» (м. Київ, 2004, 2006, 2008, 2009, 2015 рр.), Міжнародній науковій конференції «Probability, reliability and stochastic optimization» (м. Київ, 2015 р.), Міжнародній науковій конференції «XII Белорусская математическая конференция» (Білорусь, м. Мінськ, 2016 р.).

Публікації. Основні наукові результати дисертаційної роботи опубліковано в 15 наукових працях: з них 8 наукових статей [1 – 8] в наукових спеціалізованих виданнях України та інших країн (4 видання індексуються

міжнародними наукометричними базами), 7 тез доповідей на наукових та науково-практичних конференціях [9 – 15].

Структура роботи та її обсяг. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел (в кінці кожного розділу основної частини дисертації) і має 127 сторінок основного тексту, 30 рисунків, 3 таблиці, 66 сторінок додатків. Список використаних джерел містить 173 найменування і займає 18 сторінок. Загальний обсяг дисертаційної роботи – 214 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми, сформульовано мету та задачі досліджень, відображено наукову новизну і практичну значимість отриманих результатів, впровадження отриманих результатів та їх апробація.

У першому розділі проаналізовані відомі методи побудови рандомізованих симетричних шифросистем та їх практичне значення у забезпеченні безпеки державних інформаційних ресурсів. Показано, що більшість відомих методів рандомізації зводяться до певних варіантів лінійного випадкового кодування та наступного зашифровування відкритих повідомлень. Крім того, відомі методи побудови рандомізованих блокових шифросистем з нелінійним випадковим кодуванням не можуть бути безпосередньо застосовані для побудови РПШ через специфіку атак саме на потокові шифри.

При дослідженні впливу рандомізації на теоретичну стійкість захисту інформації або ключа основна увага приділяється, як правило, побудові ефективних (за різними показниками) алгоритмів рандомізації повідомлень джерела без врахування специфіки процедур наступного їх зашифровування, або сумісній побудові моделей шифрів і алгоритмів рандомізації повідомлень, що зашифровуються.

Єдиним відомим прикладом РПШ, які будуються на регулярній основі та, в принципі, можуть бути використані на практиці, є шифросистеми Міхалевича-Імаї. Рандомізатори цих шифросистем будуються на основі двійкових лінійних перетворень, зокрема, завадостійкого кодування відкритих повідомлень лінійними кодами. Проте стійкість РПШ Міхалевича-Імаї суттєво залежить від будови їх компонент і може бути значно менше, ніж стверджують їх розробники. Деякі з цих шифросистем виявляються вразливими навіть до атак на основі відомих шифрованих повідомлень і, отже, не можуть бути використані для захисту державних інформаційних ресурсів.

У другому розділі запропоновано атаки на РПШ Міхалевича-Імаї на основі відомих шифрованих повідомлень, а також підібраних векторів ініціалізації. Ці атаки дозволяють отримувати інформацію про ключ, а в окремих

випадках відновлювати ключ цілком. Оскільки обидві атаки будуються на основі загального принципу, то далі описується друга атака, що є найбільш потужною з них.

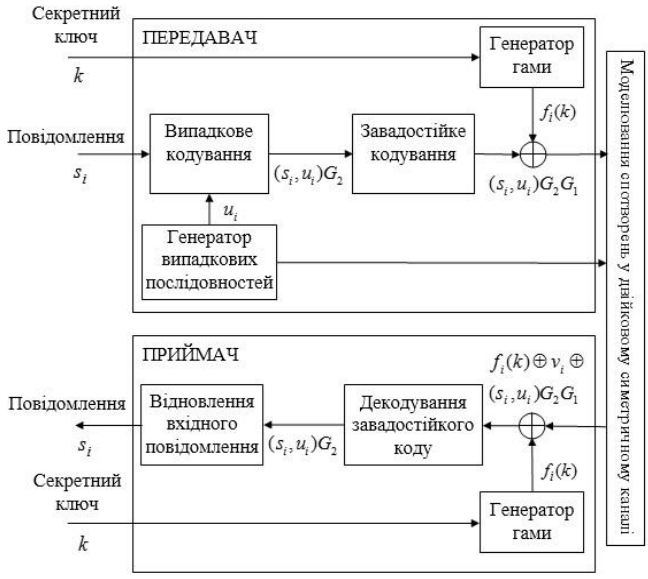

Рис. 1. Схема РПШ Міхалевича-Імаї

Позначимо V_n множину булевих векторів довжини n, $F_{m\times n}$ – множину $m\times n$-матриць над полем $F=\mathrm{GF}(2)$, $F^*_{m\times m}$ – групу оборотних матриць порядку m над цим полем. Вихідними даними для побудови РПШ Міхалевича-Імаї (рис. 1) з параметрами $l, m, n \in \mathrm{N}$, $0<p<1/2$, де $l<m<n$, та множиною ключів K є такі (несекретні) об'єкти: твірна матриця G_1 двійкового лінійного $[n, m]$-коду C_1 з ефективним алгоритмом декодування (декодером) $D: V_n \to C_1$, який дозволяє надійно виправляти помилки у двійковому симетричному каналі (ДСК) з імовірністю спотворення p; матриця $G_2 \in F^*_{m\times m}$; генератор гами, що виробляє за ключем $k \in K$ послідовність $f_0(k), f_1(k), \ldots$ двійкових векторів довжини n (при цьому вважається, що функції $f_i: K \to V_n$, $i=0,1,\ldots$, можуть залежати від загальнодоступних параметрів, наприклад, векторів ініціалізації). Для зашифровування на ключі $k \in K$ відкритого тексту $s_0, s_1, \ldots, s_t$, де $s_i \in V_l$, $i=0,1,\ldots,t$, відправник генерує послідовність незалежних випадкових векторів $u_0, v_0, u_1, v_1, \ldots, u_t, v_t$, де вектор u_i має рівномірний розподіл на множині V_{m-l}, а координати вектора v_i довжини n розподілені за законом Бернуллі з імовірністю успіху p, та обчислює шифрований текст $z_0, z_1, \ldots, z_t$ за формулою

$$z_i = (s_i, u_i)G_2G_1 \oplus f_i(k) \oplus v_i,\ i = 0, 1, \ldots, t. \qquad (1)$$

Законний одержувач, знаючи вектор $f_i(k)$, може швидко відновити повідомлення $(s_i, u_i)G_2$ за допомогою декодера D, а потім знайти вектор s_i, використовуючи оборотність матриці G_2.

Позначимо $C_0 = \{(0,u)G_2G_1 :\ u \in V_{m-l}\}$ – $[n, m-l]$-підкод коду C_1, $C_0^{\perp}$ – код, дуальний до C_0, $d_0^{\perp}$ – дуальна відстань коду C_0. При проведенні атаки на основі підібраних векторів ініціалізації супротивник виконує такий алгоритм:

1. Вибрати слово $h \in C_0^{\perp} \setminus \{0\}$ ваги $d_0^{\perp}$.

2. Подати t разів на вхід РПШ з невідомим фіксованим ключем k повідомлення $s_0 = 0$ і знайти (для вибраного $i = 0, 1, \ldots$) шифровані повідомлення

$$z^{(j)} = (0, u^{(j)})G_2G_1 \oplus f_i(k) \oplus v^{(j)},\ j \in \overline{1,t}, \qquad (2)$$

де $u^{(0)}, v^{(0)}, u^{(1)}, v^{(1)}, \ldots$ – незалежні випадкові вектори, розподілені за законами $\mathrm{P}\{u^{(j)} = u\} = 2^{-(m-l)}$, $\mathrm{P}\{v^{(j)} = v\} = p^{wt(v)}(1-p)^{n-wt(v)}$, $u \in V_{m-l}$, $v \in V_n$ (тут і далі $wt(v)$ позначає вагу Гемінга довільного вектора v);

3. Обчислити

$$z^{(j)}h^T = f_i(k)h^T \oplus v^{(j)}h^T,\ j \in \overline{1,t}, \qquad (3)$$

і відновити значення $f_i(k)h^T$ методом максимуму правдоподібності.

У розділі доведено, що для відновлення значення $f_i(k)h^T$ з системи рівнянь (3) з імовірністю $1/2 + \theta$, $0 < \theta < 1/2$, необхідно не менше ніж (4) рівнянь.

$$t_\theta = 1/4 \cdot \theta^2 (1-2p)^{-2d_0^{\perp}}. \qquad (4)$$

Також доведено, що супротивник може відновити значення $\varphi_i(k) = f_i(k)H^T$ з імовірністю не менше $1-\delta$ за $O(nt\log t)$ двійкових операцій, використовуючи $t = \left\lceil 1/2 \cdot (1-2p)^{-2d(H)} \ln(\delta^{-1}(n-m+l)) \right\rceil$ довільних рівнянь системи (2), де H – довільна перевірочна матриця коду C_0, $d(H) = \max\limits_{1 \le r \le n-m+l} wt(H_r)$, H_r – r-й рядок матриці H. Отримані оцінки показують, що запропонована атака може бути реалізована на практиці, якщо ймовірність p спотворення в ДСК є не надто великою. Зокрема, для шифросистем, побудованих на базі лінійних кодів C_0 з параметрами $n = 255$, $m - l = 185$, $d_0^{\perp} = 62$ складність атаки (з імовірністю успіху $0{,}95$) не перевищує $2^{18{,}86}$ двійкових операцій при $p = 0{,}02$ та $2^{53{,}84}$ двійкових операцій при $p = 0{,}10$.

Важливим науковим результатом розділу є загальний теоретично обґрунтований факт, що клас РПШ Міхалевича-Імаї (незалежно від будови їх компонент) володіє суттєвою слабкістю, яка полягає в зменшенні кількості інформації (в порівнянні з довжиною блоку шифрувальної гами), необхідної для відновлення за реальний час символів відкритого тексту. Зазначена властивість є наслідком спільного застосування випадкового і завадостійкого кодування повідомлень лінійними кодами та непритаманна аналогічним за будовою шифросистемам, де випадкове кодування не використовується. Так, для шифросистем, побудованих на базі лінійних кодів C_0 з параметрами $n = 255$, $m - l = 205$, $d_0^{\perp} = 62$ супротивнику потрібно знати лише 50 бітів інформації про ключ (яка міститься у векторі $\varphi_i(k) = f_i(k)H^T$) замість 255 бітів, тобто в 5 разів менше, щоб відновити відкрите повідомлення.

Окремим науковим результатом розділу є (отримані вперше) аналітичні межі для швидкості передачі інформації в рандомізованих потокових шифросистемах Міхалевича-Імаї. Нехай $M = M(G_1, G_2, p, D)$ є РПШ Міхалевича-Імаї з параметрами l, m, n, p така, що $t_\theta \ge t \ge 1$, де $\theta \in (0, 1/2)$ і t_θ визначається за (4). Тоді $\lambda_\theta(t, p) \stackrel{\text{def}}{=} -\dfrac{\log(4\theta^{-2}t)}{2n\log(1-2p)} \in (0,1)$ і якщо ймовірність p_e помилкового декодування повідомлень декодером D є такою, що $p_e + H_2(p_e) < 1$, де $H_2(\cdot)$ – двійкова ентропійна функція, то швидкість передачі інформації $\rho(M) = 1 - (m-l)/n$

$$\rho(M) \le \frac{1 - H_2(p)}{1 - p_e - H_2(p_e)} - 1 - 1/n \cdot \log\left(1 - (2\lambda_\theta(t,p))^{-1}\right), \text{ якщо } \lambda_\theta(t,p) > 1/2;$$

$$\rho(M) \le \frac{1 - H_2(p)}{1 - p_e - H_2(p_e)} - H_2\left(1/2 \cdot (1 - \sqrt{1 - 2\lambda_\theta(t,p) + 2/n}) - 1/n\right) + \log(n\sqrt{n})/n,$$

якщо $1/n < \lambda_\theta(t,p) \le 1/2$.

Застосування отриманих меж до рандомізованих потокових шифросистем з параметром $n = 512$ показує, що їх стійкість не перевищує 2^{79} операцій (якими б не були їх компоненти).

При передачі повідомлень зі швидкістю 0,36 максимальне значення стійкості шифросистеми не перевищує 2^{20} операцій, а збільшення швидкості до 0,5 призводить до втрати стійкості (рис. 2). Зазначені факти свідчать про обмежені можливості РПШ Міхалевича-Імаї з погляду сучасних вимог щодо стійкості та практичності в реальних умовах.

У третьому розділі викладено альтернативний метод побудови РПШ з підвищеною стійкістю, сутність якого полягає в застосуванні для випадкового кодування нелінійних відображень або безключових геш-функцій.

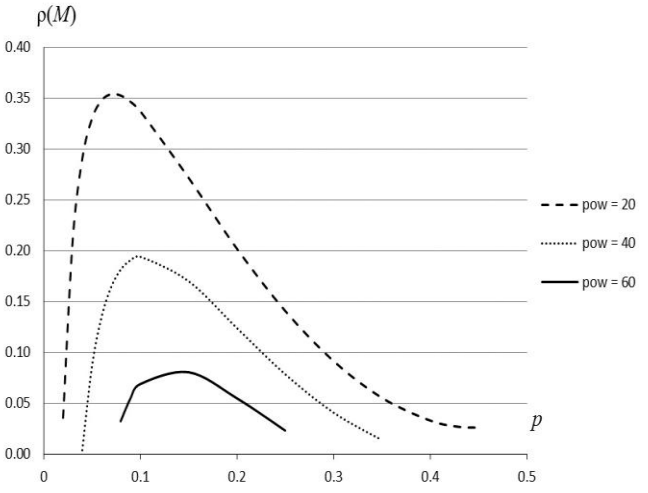

Рис. 2. Залежності верхніх оцінок швидкості передачі інформації у РПШ Міхалевича-Імаї від імовірності спотворення у ДСК

На відміну від раніше відомих, запропонований метод надає більше можливостей для побудови обчислювально стійких РПШ за рахунок розширення класу перетворень, що використовуються в конструкції рандомізатора.

За означенням вхідними даними для побудови РПШ з нелінійним випадковим кодуванням з параметрами $l, m \in \mathrm{N}$, де $l < m$, та множиною ключів K є такі об'єкти: відображення $\phi : V_{m-l} \to V_l$; комутативна групова операція $*$ на множині V_m; підстановочна матриця P порядку m; генератор гами, який виробляє за ключем $k \in K$ послідовність булевих векторів довжини m. Аналогічно РПШ Міхалевича-Імаї вважається, що функції $f_i : K \to V_m$, $i = 0, 1, \ldots$, можуть залежати від загальнодоступних параметрів (векторів ініціалізації).

Для зашифровування на ключі $k \in K$ відкритого тексту $s_0, s_1, \ldots, s_t$, де $s_i \in V_l$, $i = 0, 1, \ldots, t$, відправник генерує послідовність незалежних випадкових рівноймовірних векторів $u_0, u_1, \ldots, u_t$ довжини $m - l$ та обчислює шифрований текст $z_0, z_1, \ldots, z_t$ за формулою

$$z_i = (u_i, s_i \oplus \phi(u_i))P * f_i(k), \; i = 0, 1, \ldots, t. \qquad (5)$$

Законний одержувач, маючи вектор $f_i(k)$, може обчислити повідомлення $(z_{1,i}, z_{2,i}) = z_i *^{-1} f_i(k)$, де $z_{1,i} \in V_{m-l}$, $z_{2,i} \in V_l$, а операція $*^{-1}$ визначається таким співвідношенням: $x = y *^{-1} z \Leftrightarrow y = x * z$, $x, y, z \in V_m$. Після цього він може відновити повідомлення s_i за формулою $s_i = \phi(z_{1,i}) \oplus z_{2,i}$. При цьому супротивник для знаходження ключа k вимушений мати справу зі спотвореною гамою $(u_i, s_i \oplus \phi(u_i))P * f_i(k)$, $i = 0, 1, \ldots, t$.

Вхідні дані $\phi, *, P$ слід вибирати з урахуванням вимог як до криптографічної

стійкості, так і ефективності реалізації перетворень вигляду (5). Відображення ϕ слід вибирати більш ретельно, оскільки його властивості суттєвим чином впливають на стійкість шифросистеми, що розглядається.

Пропонується використовувати один із двох загальних підходів: 1) застосовувати в ролі ϕ нелінійне відображення множини V_l (при $m = 2l$) з гарними криптографічними властивостями на зразок тих, що використовуються в сучасних блокових шифрах; 2) застосовувати в ролі ϕ безключову геш-функцію (таку як Keccak або «Купина»). Враховуючи той факт, що стійка геш-функція достатньо добре імітує випадкове відображення (в даному випадку множини V_{m-l} в множину V_l), останній варіант видається більш переважним з погляду забезпечення належної стійкості рандомізованої шифросистеми.

У цьому розділі отримано аналітичні оцінки параметрів, що характеризують обчислювальну стійкість запропонованих шифросистем відносно атак, подібних тим, які будуються для шифросистем Міхалевича-Імаї. Наслідком отриманих результатів є встановлені вимоги до відображення $\phi : V_{m-l} \to V_l$:

1. Велике значення параметра $m-l$ для протидії перебірній атаці, яка полягає у розв'язанні системи рівнянь вигляду $(u_j, \phi(u_j))P * f_i(k) = y_j$, $j = \overline{1,t}$, де значення $y_1, y_2, \ldots, y_t$ є відомими, а значення $f_i(k)$, $u_1, \ldots, u_t$ невідомі (доведено, що істинний розв'язок цієї системи рівнянь можна знайти з імовірністю не менше $1-\delta$ за $O\left(2^{m-l}\left(1+\frac{\log \delta^{-1}}{m-l}\right)\right)$ операцій при $\delta \to 0$ та $m-l \to \infty$).

2. Мале значення параметра $L_\phi = \max\limits_{a \in V_{m-l},\, b \in V_l \setminus \{0\}} \{|1-2l_\varphi(a,b)|\}$, де $l_\phi(a,b) = 2^{-(m-l)} |\{z \in V_{m-l} : az \neq b\phi(z)|$, для протидії атаці лінійного типу. Зазначена атака полягає у розв'язанні для кожного $r \in \overline{1,m}$ системи рівнянь

$$(a_r u_j \oplus b_r \phi(u_j)) \oplus (a_r, b_r) f_i(k) = (a_r, b_r) y_j, \quad j = \overline{1,t}, \tag{6}$$

де (a_r, b_r) – лінійно незалежні вектори ($a_r \in V_{m-l}$, $b_r \in V_l \setminus \{0\}$) такі, що $l_\phi(a_r, b_r) \neq 1/2$, $r \in \overline{1,m}$ (доведено, що для відновлення значення $(a_r, b_r) f_i(k)$ з системи рівнянь (6) з імовірністю $1/2 + \theta$, $\theta \in (0, 1/2)$, необхідно не менше ніж $t_\theta = 1/4 \cdot \theta^2 \cdot L_\phi^{-2}$ рівнянь).

3. Велика часова складність розв'язання системи рівнянь

$$\phi(z \oplus (\alpha_1 \oplus \alpha_j)) \oplus \phi(z) = \beta_1 \oplus \beta_j, \quad j = \overline{2,t}, \tag{7}$$

для довільних (відомих) векторів α_j, β_j, $j = \overline{1,t}$.

При цьому, для підвищення практичності РПШ величина l повинна бути також достатньо великою (наприклад, умова $m - l = l = 128$ забезпечує швидкість передачі інформації $l/m = 1/2$ незалежно від вибору відображення ϕ).

У четвертому розділі виконано порівняння запропонованих шифросистем з шифросистемами Міхалевича-Імаї за стійкістю (при фіксованій швидкості передачі) та швидкістю передачі (при фіксованій стійкості) при однаковій довжині шифрованих повідомлень. Крім того, розроблено програмні реалізації трьох варіантів РПШ з нелінійним випадковим кодуванням, що дозволяють здійснювати на практиці процедури зашифровування/розшифровування даних в режимі реального часу.

Результати порівняння РПШ наведено в табл. 1, з якої видно, що для кожного з трьох значень параметра n стійкість РПШ з нелінійним випадковим кодуванням є суттєво вище стійкості РПШ Міхалевича-Імаї, які виявляються практично нестійкими при зазначеній швидкості передачі 1/2. Зокрема, при $n = 512$ і $n = 1024$ стійкість РПШ з нелінійним випадковим кодуванням вища за стійкість РПШ Міхалевича-Імаї у 2^{242} і 2^{487} разів відповідно.

Таблиця 1

Межі максимальної стійкості РПШ при заданих обмеженнях щодо швидкості передачі ($l/n = 1/2$) та довжини шифрованих повідомлень ($p_e = 10^{-8}$, $\theta = 0{,}45$)

Довжина n шифрованого повідомлення	Двійковий логарифм верхньої межі інформаційної складності атаки на РПШ Міхалевича-Імаї	Двійковий логарифм нижньої межі інформаційної складності атаки на РПШ з нелінійним випадковим кодуванням
256	2	121
512	7	249
1024	18	505

З метою оцінки на практиці ефективності РПШ з нелінійним випадковим кодуванням розроблено та програмно реалізовано конкретні варіанти шифросистем. Показано, що побудовані рандомізовані потокові шифросистеми можуть бути застосовані на практиці для зашифровування/розшифровування даних в режимі реального часу. Реалізації зазначених шифросистем виконано у таких варіантах (ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ – ВІДОБРАЖЕННЯ ϕ – ГЕНЕРАТОР ГАМИ): «Isaac – Keccak – Snow 2.0» (IKCS); «Isaac – «Купина» – Snow 2.0» (IKPS); «Isaac – NonLinearMap – Snow 2.0» (INLS), де елемент NonLinearMap означає нелінійне відображення $\varphi(x) = x^{2^{l/2+l/4+1}}$, $x \in \mathrm{GF}(2^l)$. В ко-

жному з трьох варіантів реалізацій вибрано такі значення параметрів: $l = 256$, $m = 512$. Криптографічна схема першого варіанту реалізації рандомізованої потокової шифросистеми з нелінійним випадковим кодуванням наведена на рис. 3. Решта варіантів будуються аналогічним чином. Крім того, з використанням пакету OpenSSL реалізовано алгоритм AES в режимі зворотного зв'язку за виходом.

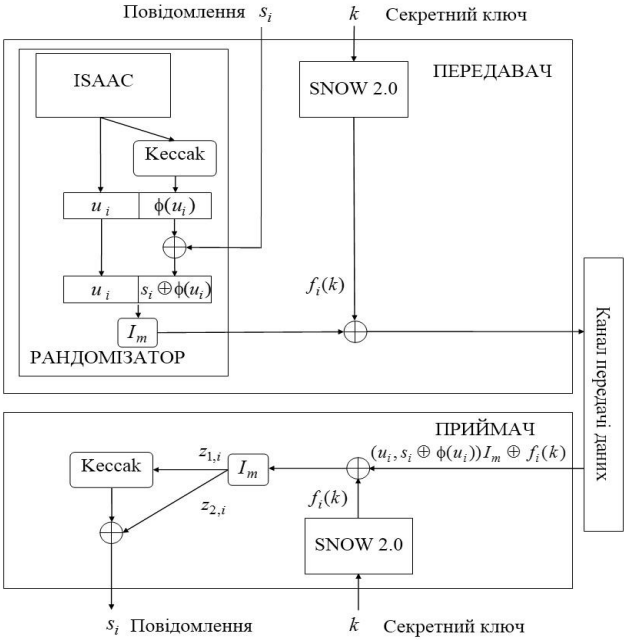

Рис. 3. Схема РПШ з нелінійним випадковим кодуванням IKCS

Час виконання процедур зашифровування/розшифровування повідомлень з використанням розроблених реалізацій рандомізованих потокових шифросистем з нелінійним випадковим кодуванням наведені в табл. 2. Всі реалізації виконувались на обчислювальній системі з процесором Intel(R) Core(TM) i3-6100, 3.7GHz та обсягом оперативної пам'яті 4 ГБ на базі 64-розрядної операційної системи Windows 7 Service Pack 1. Мова програмування – C++. Середовище розробки – Microsoft Visual Studio 2013 (Release версія). Як видно з таблиці, найбільш ефективною серед РПШ за часом виконання процедур зашифровуваня/розшифровування виявляється РПШ IKCS, в якій відображення ϕ реалізовано геш-функцією Keccak. Стійкість РПШ INLS відносно найбільш потужної на сьогодні атаки на основі підібраних векторів ініціалізації є не менше ніж 2^{249} операцій (див. табл. 1).

В цілому, отримані результати свідчать про помітну перевагу (як з погляду стійкості, так і практичності) побудованих РПШ в порівнянні з рандомізованими потоковими шифросистемами Міхалевича-Імаї.

Таблиця 2

Типовий приклад, що ілюструє час виконання процедур зашифровування/розшифровування для РПШ з нелінійним випадковим кодуванням та алгоритму AES

Довжина файлу даних	IKCS	IKPS	INLS	AES
Файл 1 – 3454 б	0,011 сек.	0,152 сек.	0,735 сек.	0,001 сек.
Файл 2 – 180 Кб	0,106 сек.	6,905 сек.	32,160 сек.	0,016 сек.
Файл 3 – 1162 Кб	0,526 сек.	45,122 сек.	208,228 сек.	0,023 сек.

У висновках викладено найбільш важливі наукові та практичні результати дисертаційного дослідження, сформульовано розв'язану наукову задачу, розкрито методи її розв'язання, наукове та практичне значення роботи, обґрунтованість та достовірність отриманих результатів, подано висновки та рекомендації щодо їхнього подальшого використання.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу й актуальну *наукову задачу* розробки методу побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням для забезпечення безпеки державних інформаційних ресурсів.

1. Проведено детальний аналіз доступних наукових публікацій щодо рандомізованих шифросистем для забезпечення безпеки державних інформаційних ресурсів. З'ясовано, що більшість відомих методів побудови рандомізованих шифросистем зводиться до певних варіантів лінійного випадкового кодування та наступного зашифровування відкритих повідомлень. Крім того, відомі методи побудови рандомізованих блокових шифросистем з нелінійним випадковим кодуванням не можуть бути безпосередньо застосовані для побудови РПШ через специфіку атак саме на потокові шифри. Єдиним відомим прикладом РПШ, які будуються на регулярній основі та можуть бути використані на практиці, є РПШ Міхалевича-Імаї, однак стійкість цих шифросистем суттєво залежить від будови їх компонент і може бути значно менше, ніж стверджують їх розробники.

2. Розроблено атаку на РПШ Міхалевича-Імаї на основі підібраних векторів ініціалізації, що має обчислювальну складність, яка залежить лінійно від довжини кодового слова та субквадратично від обсягу матеріалу, що використовується. Для шифросистем, побудованих на базі лінійних кодів C_0 з параметрами $n = 255$, $m - l = 185$, $d_0^{\perp} = 62$ складність атаки (з імовірністю успіху $0{,}95$) не перевищує $2^{18{,}86}$ двійкових операцій при $p = 0{,}02$ та $2^{53{,}84}$ двійкових операцій при $p = 0{,}10$.

3. Суттєва слабкість класу РПШ Міхалевича-Імаї в цілому полягає в зменшенні кількості інформації (в порівнянні з довжиною блоку шифруваль-

ної гами), що необхідна для відновлення за реальний час символів відкритого тексту. Зазначена властивість є наслідком спільного застосування випадкового і завадостійкого кодування повідомлень лінійними кодами та непритаманна аналогічним за будовою шифросистемам, де випадкове кодування не використовується.

4. Отримані аналітичні межі для швидкості передачі інформації в РПШ Міхалевича-Імаї дозволяють з'ясувати їх потенційні можливості та визначити загальні обмеження, яким задовольняють окремі показники їх ефективності при заданих значеннях інших показників. Застосування отриманих меж до РПШ з параметром $n=512$ показує, що їх стійкість не перевищує 2^{79} операцій (якими б не були їх компоненти). При передачі повідомлень зі швидкістю $0{,}36$ максимальне значення стійкості шифросистеми не перевищує 2^{20} операцій, а збільшення швидкості до $0{,}5$ призводить до втрати стійкості. Зазначені факти свідчать про обмежені можливості РПШ Міхалевича-Імаї з погляду сучасних вимог щодо стійкості та практичності в реальних умовах.

5. Запропонований метод побудови РПШ з нелінійним випадковим кодуванням базується на застосуванні для випадкового кодування нелінійних відображень або безключових геш-функцій і надає більше можливостей для побудови обчислювально стійких шифросистем за рахунок розширення класу перетворень, що використовуються в конструкції рандомізатора. Обчислювальна стійкість запропонованих РПШ відносно найбільш потужних (з відомих сьогодні) атак на основі підібраних векторів ініціалізації визначається такими властивостями відображення $\phi: V_{m-l} \to V_l$: велике значення параметра $m-l$ для протидії перебірній атаці; мале значення параметра L_ϕ для протидії атакам лінійного типу; велика часова складність розв'язання системи рівнянь (7). На відміну від РПШ Міхалевича-Імаї, що є вразливими до кореляційних атак (або малопрактичними), запропоновані РПШ є обчислювально стійкими відносно атаки на основі підібраних векторів ініціалізації, якщо відображення ϕ характеризується малим значенням максимального елемента таблиці лінійних апроксимацій. При цьому, для підвищення практичності РПШ величина l повинна бути також достатньо великою (наприклад, умова $m-l=l=128$ забезпечує швидкість передачі інформації $l/m=1/2$ незалежно від вибору відображення ϕ). Для шифросистем, побудованих на базі відображень $\phi: V_{m-l} \to V_l$ з параметрами $l=128$, $m=256$, обчислювальна стійкість відносно перебірної атаки складає 2^{134} операцій, якщо параметр D_ϕ дорівнює 2^{-2} та 2^{130} операцій, якщо цей параметр дорі-

внює 2^{-120}. Якщо при цьому $L_{\phi} = 2^{-61}$, то обчислювальна стійкість зазначених шифросистем відносно атаки лінійного типу складає 2^{127}.

6. Результати порівняння стійкості двох зазначених видів РПШ при фіксованій швидкості передачі свідчать про суттєву перевагу запропонованих РПШ над РПШ Міхалевича-Імаї, які виявляються практично нестійкими при зазначеній швидкості. Зокрема, при $n = 512$ і $n = 1024$ стійкість РПШ з нелінійним випадковим кодуванням вища за стійкість РПШ Міхалевича-Імаї у 2^{242} і 2^{487} разів відповідно. Аналіз вибору компонент для практичної побудови конкретних варіантів РПШ з нелінійним випадковим кодуванням показує, що в ролі нелінійного відображення в конструкції рандомізатора доцільно використовувати одну з відомих обчислювально стійких геш-функцій, наприклад «Купину» або Keccak. Побудовані таким чином РПШ є безумовно стійкими відносно будь-яких атак на основі підібраних векторів ініціалізації в моделі випадкового оракула та забезпечують практичну стійкість на рівні 2^{l} операцій за умови практичної стійкості геш-функції Keccak-l та «Купина»-l. Розроблені програмні реалізації трьох варіантів РПШ з нелінійним випадковим кодуванням дозволяють на практиці здійснювати зашифровування/розшифровування даних в режимі реального часу. При цьому найбільш ефективною за часом виконання процедур зашифровування/розшифровування є шифросистема IKCS (ISAAC – Keccak –Snow 2.0). Зокрема, час зашифровування/розшифровування файлів розміром 180 Кб за допомогою цієї шифросистеми є в 65 та 303 рази менше часу зашифровування/розшифровування файлів такого ж розміру за допомогою шифросистем IKPS та INLS відповідно.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. А.Н. Алексейчук, С.В. Гришаков, «Нелинейное случайное кодирование в системах передачи информации по каналу связи с отводом», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, В. 8, С. 133-140, 2004.

2. А.Н. Алексейчук, С.В. Гришаков, «Алгоритмы нелинейного случайного кодирования и декодирования сообщений Z_4-линейными кодами в модели wire-tap channel», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, В. 2(13), С. 169-176, 2006.

3. А.Н. Алексейчук, С.В. Гришаков, «Неасимптотические оценки эффективности случайного кодирования в системе передачи информации по двоичному симметричному каналу связи с отводом», *Системні дослідження та інформаційні технології*, № 4, С. 37-47, 2011.

4. A.M. Alekseychuk, S.V. Gryshakov, «On the computational security of randomized stream ciphers proposed by Mihalević and Imai», *Захист інформації*, Т. 16, № 4, С. 328-334, 2014.

5. А.М. Олексійчук, С.В. Гришаков, «Метод побудови рандомізованих потокових шифросистем на основі нелінійного випадкового кодування», *Спеціальні телекомунікаційні системи та захист інформації*, В. 2(26), С. 5-14, 2014.

6. A. Alekseychuk, S. Gryshakov, «Randomized stream ciphers with enhanced security based on nonlinear random coding», *Journal of Mathematics and System Science*, V.5, pp. 516-522, 2015.

7. А.Н. Алексейчук, С.В. Гришаков, «Границы для скорости передачи информации в рандомизированных поточных шифрсистемах Михалевича-Имаи», *Радиотехника*, В. 181, С. 31-39, 2015.

8. А.Н. Алексейчук, С.В. Гришаков, «Стойкие и практичные рандомизированные поточные шифры на основе кодов Рида-Соломона», *Кибернетика и системный анализ*, Т. 53, № 2, С. 114-121, 2017.

9. А. Алексейчук, С. Гришаков, «Нелинейное случайное кодирование в системах передачи информации по каналу связи с отводом», *Безпека інформації у інформаційно-телекомунікаційних системах*: *тези доп. VII міжнар. наук.-практ. конф*., 12-14 травня 2004 р., К., 2004, С. 25.

10. А. Алексейчук, С. Гришаков, «Алгоритмы случайного кодирования Z_4-линейными кодами в системе передачи информации по каналу связи с отводом», *Безпека інформації у інформаційно-телекомунікаційних системах: тези доп. IX міжнар. наук.-практ. конф*., 17-19 травня 2006 р., К., 2006, С. 19.

11. А. Алексейчук, С. Гришаков, «Оценки стойкости защиты многократно переданных сообщений в модели WTC», *Безпека інформації у інформаційно-телекомунікаційних системах: тези доп. XI міжнар. наук.-практ. конф*., 20-22 травня 2008 р., К., 2008, С. 31.

12. А. Алексейчук, С. Гришаков, «Оценки характеристик эффективности системы передачи информации по каналу связи с отводом в случае неидеального основного канала», *Безпека інформації у інформаційно-телекомунікаційних системах: тези доп. XII міжнар. наук.-практ. конф*., 19-21 травня 2009 р., К., 2009, С. 26.

13. A.N. Alekseychuk, S.V. Gryshakov, «Randomized stream ciphers with enhanced security based on nonlinear random coding», *Probability, reliability and stochastic optimization (PRESTO 2015)*, Proceedings, April 7-10, Kyiv, Ukraine, 2015, pp. 27.

14. А. Олексійчук, С. Гришаков, «Рандомізовані шифросистеми Міхалевича-Імаї на основі кодів Ріда-Соломона», *Безпека інформації у інформаційно-телекомунікаційних системах: тези доп. XVII міжнар. наук.-практ. конф*., 26-28 травня 2015 р., К., 2015, С. 27.

15. А.Н. Алексейчук, С.В. Гришаков, «Стойкие и практичные рандомизированные поточные шифры на основе кодов Рида-Соломона», *XII Белорусская математическая конференция*, 5-10 сентября 2016 г., Минск, Беларусь, С.28.

АНОТАЦІЯ

Гришаков С.В. Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – Інформаційна безпека держави. – Національний авіаційний університет, Київ, 2018.

У дисертації розв'язано актуальну наукову задачу розробки методу побудови рандомізованих потокових шифросистем (РПШ) з нелінійним випадковим кодуванням для забезпечення безпеки державних інформаційних ресурсів. Вперше отримано аналітичні оцінки параметрів, що визначають стійкість РПШ Міхалевича-Імаї відносно атак на основі відомих шифрованих повідомлень, а також підібраних векторів ініціалізації. Вперше доведено, що клас РПШ Міхалевича-Імаї володіє суттєвою слабкістю, яка полягає в зменшенні кількості інформації, що необхідна для відновлення за реальний час символів відкритого тексту. Вперше отримано аналітичні межі для швидкості передачі інформації в РПШ Міхалевича-Імаї при заданих обмеженнях щодо ймовірності правильного прийому повідомлень законним користувачем та стійкості шифрування. Отримав подальший розвиток метод побудови РПШ, який, на відміну від раніше відомих, базується на застосуванні для випадкового кодування нелінійних відображень або безключових геш-функцій. Отримані нові наукові результати надають розробникові більше можливостей для побудови обчислювально стійких РПШ за рахунок розширення класу перетворень, що використовуються в конструкції рандомізатора. Головним практичним результатом роботи є можливість на практиці будувати обґрунтовано стійкі РПШ без внесення змін в алгоритми шифрування для забезпечення безпеки державних інформаційних ресурсів.

Ключові слова: безпека державних інформаційних ресурсів, потоковий шифр, випадкове кодування, методи побудови рандомізованих потокових шифросистем, обчислювальна стійкість, обґрунтування стійкості.

АННОТАЦИЯ

Гришаков С.В. Метод построения рандомизированных поточных шифрсистем с нелинейным случайным кодированием. – Рукопись.

Диссертация на соискание научной степени кандидата технических наук по специальности 21.05.01 – Информационная безопасность государства. – Национальный авиационный университет, Киев, 2018.

В диссертации решена актуальная научная задача разработки метода построения рандомизированных поточных шифрсистем (РПШ) с нелинейным случайным кодированием для обеспечения безопасности государственных информационных ресурсов.

В первом разделе проанализированы известные методы построения рандомизированных симметричных шифрсистем и их практическое значение в обеспечении безопасности государственных информационных ресурсов. На основе проведенного анализа доступных научных публикаций показано, что большинство известных методов построения рандомизированных шифрсистем сводятся к некоторым вариантам линейного случайного кодирования и последующего зашифровывания открытых сообщений. Единственным примером РПШ, которые строятся на регулярной основе и, в принципе, могут быть использованы на практике, являются шифрсистемы Михалевича-Имаи.

Во втором разделе проведен анализ вычислительной стойкости РПШ Михалевича-Имаи относительно различных атак (в частности, предложенных впервые). Показано, что стойкость этих шифрсистем существенно зависит от строения их компонент и может быть значительно меньше, чем утверждают их разработчики. В частности, некоторые из указанных РПШ являются уязвимыми даже к атакам на основе известных шифрованных сообщений. Кроме того, в разделе получены аналитические границы для скорости передачи информации в РПШ Михалевича-Имаи при заданных ограничениях относительно вероятности правильного приема сообщений законным получателем и стойкости шифрования. Полученные результаты свидетельствуют об ограниченных возможностях РПШ Михалевича-Имаи с точки зрения современных требований к стойкости и практичности в реальных условиях.

В третьем разделе предложен метод построения РПШ с нелинейным случайным кодированием, суть которого состоит в применении для случайного кодирования нелинейных отображений или безключевых хэш-функций. Получены аналитические оценки стойкости предложенных шифрсистем относительно атак на основе известных шифрованных сообщений, а также относительно наиболее мощных (на сегодня) атак на основе подобранных векторов инициализации. Приведены рекомендации по выбору компонент для построения рандомизаторов указанных шифрсистем.

В четвертом разделе проведено сравнение стойкости (при фиксированной скорости передачи) и скорости передачи (при фиксированной стойкости) РПШ Михалевича-Имаи и РПШ с нелинейным случайным кодированием. Полученные результаты показывают, что РПШ с нелинейным случайным кодированием являются более стойкими (в 2^{242} и более раз) и более скоростными (в 125 и более раз), чем шифрсистемы Михалевича-Имаи при одинаковой длине вы-

ходного сообщения. Кроме того, разработаны программные реализации шифрсистем с нелинейным случайным кодированием на основе обоснованного выбора их компонент. Показано, что построенные шифрсистемы могут быть использованы на практике для зашифровывания/расшифровывания данных в режиме реального времени.

В целом, полученные новые научные и практические результаты имеют универсальный характер и позволяют строить обоснованно стойкие РПШ без внесения изменений в алгоритмы шифрования для обеспечения безопасности государственных информационных ресурсов.

Ключевые слова: безопасность государственных информационных ресурсов, поточный шифр, случайное кодирование, методы построения рандомизированных поточных шифрсистем, вычислительная стойкость, обоснование стойкости.

ABSTRACT

Gryshakov S.V. Method for designing randomized stream ciphers with nonlinear random coding. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 21.05.01 – Information security of the state, National Aviation University, Kyiv, 2018.

This thesis is devoted to solving actual scientific problem of development the method for designing randomized stream ciphers (RSC) with nonlinear random coding to provide the security of state information resources. Analytical estimates of the parameters that determine the security of the Mihalević-Imai RSC against known ciphertext attacks and chosen initialization vectors attacks are obtained in the thesis for the first time. It was proved for the first time that a class of the Mihalević-Imai RSC has a significant weakness which consists in reducing the amount of information which is necessary for real-time recovery of the plaintext. Analytical bounds of the transmission rate for the Mihalević-Imai RSC given the limitations on the encryption security and the probability of the correct reception of messages by the legitimate receiver are obtained for the first time. The technique for designing RSC was further developed. In contrast to before known approaches, the proposed method is based on the employment of the nonlinear transformations or keyless hash functions for random coding. Obtained new scientific results give the developer more capabilities for designing computationally secure RSC by enlarging the class of transformations used in the construction of a randomizer. Main practical result of the thesis is a possibility to design provably secure RSC without changing the encryption algorithms to ensure the security of state information resources.

Key words: security of state information resources, stream cipher, random coding, methods for designing randomized stream ciphers, computational security, security proving.