

Харьковский национальный университет радиоэлектроники

Академия наук прикладной радиоэлектроники

ПРИКЛАДНАЯ РАДИОЭЛЕКТРОНИКА

Научно-технический журнал

И.о. главного редактора

Чурюмов Г.И.

Зам. главного редактора

Дохов А.И.

Редакционный совет

Гузь В.И., Довбня А.Н., Егоров А.М., Калугин В.В., Кравченко В.И.,
Назаренко И.П. (Россия), Неклюдов И.М., Пресняк И.С., Симонов К.Г. (Россия),
Симанков В.С. (Россия), Слипченко Н.И., Чабдаров Ш.М. (Россия),
Яковенко В.М., Ярошенко В.С. (Россия)

Редакционная коллегия

Абрамович Ю.И. (США), Бодянский Е.В., Борисов А.В., Буц В.А., Бых А.И.,
Гомозов В.И., Жуйков В.Я., Зарицкий В.И., Кипенский А.В., Кульпа К. (Польша),
Леховицкий Д.И., Литвинов В.В., Лукин К.А., Мачехин Ю.П.,
Модельский Й. (Польша), Нерух О.Г., Поляков Г.А., Ролинг Г. (Германия),
Седышев Ю.Н., Серков А.А., Сухаревский О.И., Чурюмов Г.И.,
Шифрин Я.С., Шкварко Ю.В. (Мексика)

Адрес редакции:

Редакция журнала «Прикладная радиоэлектроника»
Харьковский национальный университет радиоэлектроники
просп. Ленина, 14, 61166, Харьков, Украина
Тел.: + 38 (057) 702 10 57
Факс: + 38 (057) 702 10 13
E-mail: are@kture.kharkov.ua
<http://www.anpre.org.ua>

СОДЕРЖАНИЕ

МЕТОДЫ СИНТЕЗА И АНАЛИЗА СИММЕТРИЧНЫХ ШИФРОВ

Конюшок С.М., Олексійчук А.М., Сторожук А.Ю. Швидкий імовірнісний алгоритм оцінювання відстані між зрівноваженою булевою функцією та множиною k -вимірних функцій	186
Oliyunkov R., Kaidalov D. Related-key cryptanalysis of perspective symmetric block cipher	192
Кузнецов А.А., Иваненко Д.В., Колованова Е.П. Моделирование перспективного блочного шифра «Калина»	201
Лисицкий К.Е. Снова об оптимальных S-блоках	208
Горбенко И.Д., Долгов В.И., Лисицкий К.Е. Уточнённые показатели прихода шифров к состоянию случайной подстановки	213
Тімохін С.С., Горбенко І.Д. Дослідження та порівняльний аналіз перспективних поточкових шифрів	217
Долгов В.И., Лисицкая И.В., Лисицкий К.Е. Новый взгляд на шифр Мухомор	221
Кузнецов О.О., Иваненко Д.В., Колованова Е.П. Аналіз колізійних властивостей режиму вироблення імітовставок із вибіркоким гамуванням	226
Руженцев В.И. Вероятности двухцикловых дифференциалов g_{ijndael} -подобного шифра с произвольными подстановками	235
Кузнецов О.О., Горбенко Ю.І., Колованова Е.П. Періодичні властивості шифргами у режимі output feedback	239

ЭЛЕКТРОННЫЕ ДОВЕРИТЕЛЬНЫЕ УСЛУГИ И ИХ РЕАЛИЗАЦИЯ

Потий А.В., Горбенко Ю.И., Корнейко А.В., Козлов Ю.Н., Пушкарев А.И., Горбенко И.Д. EIDAS: Принципы предоставления доверительных электронных услуг и проблема интероперабельности	252
Горбенко Ю.И., Потий А.В., Костенко А.В., Исирова Е.В., Горбенко И.Д. Состояние и сущность процессов нормализации Европейской нормативной базы в области электронных подписей	261
Горбенко Ю.І., Ганзя Р.С. Аналіз стійкості постквантових криптосистем	268
Гончарова Ю.В., Ерёмченко А.А. STORK — перспективный проект европейской транснациональной электронной идентификации	275
Качко Е.Г., Балагура Д.С., Погребняк К.А. Влияние свойств современных процессоров на производительность программ	281

КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ОЦЕНКА

Бессалов А.В. Построение кривой Эдвардса на базе изоморфной эллиптической кривой в канонической форме	286
Єсіна М.В., Горбенко І.Д., Бакликов О.О. Пароль як фактор багатофакторної автентифікації	290
Бойко А.О. Метод протидії перебору паролів, що не створює вразливості порушення доступності	296
Погребняк К.А., Денисов Д.С. Загальна атака на NTRUEncrypt на основі помилок розшифрування	298
Гриненко Т.А., Нарезжний А.П. Применение кодов аутентификации сообщений для обнаружения модификаций данных в региональных системах дифференциальной коррекции навигационных сигналов систем GPS/ГЛОНАСС	301

МЕТОДЫ И МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Потий А.В., Комин Д.С., Козлов Ю.Н. Классификация методов обеспечения доверия к безопасности продуктов и систем информационных технологий	311
Торба А.А., Бобух В.А., Бобкова А.А. Быстродействующий детерминированный генератор псевдослучайных последовательностей для потокового шифрования	316
Горбачев В.А. Достаточные условия безопасности информации в электронных системах	319
Ленишин А.В. Метод проектування та верифікації функцій комплексів засобів захисту від несанкціонованого доступу	328
Горбенко І.Д., Харламб М.І. Порівняльний аналіз стандартизованих версій криптоалгоритму ECIES	333
Броншпак Г.К., Громыко И.А., Доценко С.И., Перчик Е.Л. Криптография нового поколения: интегральные уравнения как альтернатива алгебраической методологии	337
Онацький О.В. Методологія створення комплексної системи захисту інформації	350
Рома О.М., Белас О.М., Ніколаєнко Б.А. Імітаційна модель оцінки завадостійкості квазікогерентної демодуляції OFDM-сигналу під час обробки «в цілому»	357

Памяти Алмазова Владислава Борисовича (11.10.1932–04.10.2014)	364
---	-----

УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Настоящий выпуск журнала «Прикладная радиоэлектроника» является тематическим и посвящен проблемным вопросам информационной безопасности и криптографической защиты информации. Представленные в журнале статьи в основном являются заказными, тематика которых определяется практическими приложениями. В основном они подготовлены специалистами по тематике, ориентируясь на задачи, которые решаются спонсором издания журнала — ПАТ «Институт информационных технологий», г. Харьков. Важное внимание уделяется проблемным вопросам создания системы электронных доверительных трансграничных услуг.

В первом разделе представлен ряд статей, посвященных проблемным вопросам синтеза и анализа симметричных криптопреобразований. В основном статьи посвящены симметричным криптографическим преобразованиям типа блочные симметричные шифры (БСШ). В этом направлении остаются актуальными и требующие разрешения задачи доказательства стойкости, оптимизации по критериям криптографическая стойкость — сложность, в первую очередь скорость преобразования. При этом тематика статей носит в основном проблемный теоретический характер, но в тоже время направлены на решение конкретных практических задач — анализа и синтеза перспективных БСШ, а также оценки существующих, в первую очередь закреплённых в стандартах.

Второй раздел посвящен задачам предоставления трансграничных электронных доверительных услуг. В качестве основы рассматриваются решения и требования, которые сегодня закреплёны в Регламентах Европейского Союза, соответственно 2012 и 2014 годов. Важными в этом направлении являются задачи и их анализ, которые направлены на выполнение требований «Регламента Европейского Парламента и Совета относительно электронной идентификации трансовых сервисов электронных операций на внутреннем рынке».

В плане решения указанных задач важные результаты получены в научно-техническом проекте ЕС STORK и STORK 2.0. Поэтому их анализ, на наш взгляд, а также определения задач для Украины, являются актуальными и необходимыми, требующими своего разрешения. Также важными, с точки зрения практики, являются задачи нормализации Европейской нормативной

базы в области электронных подписей. В первую очередь относительно схемы нумерации документов ЭЦП, а также предметные области их применения.

В третьем разделе в основном представлены статьи, посвященные криптоанализу асимметричных криптографических систем, построению общесистемных параметров, оценке стойкости многофакторных систем защиты от НСД, а также оценке стойкости систем криптографических преобразований в фактор-кольце. Значительный интерес представляет статья, посвященная необходимости применения кодов аутентификации сообщений (MAC) для обеспечения целостности и достоверности корректирующей информации, формируемой системами дифференциальной коррекции навигационных сигналов систем GPS/ГЛОНАСС.

В четвертом разделе собраны статьи, направленные на решение общих и частных задач защиты информации. Важными и актуальными, на наш взгляд, являются результаты исследования относительно:

- классификации методов обеспечения доверия к безопасности продуктов и систем информационных технологий;
- субъектно-объектной модели доступа и аксиоматически необходимым условиям защищенности информации;
- подходов к созданию и использованию шаблонов для алгоритмов создания и применения услуг безопасности для формальной нотации;
- сравнительного анализа версий криптопротоколов ECIES.

Также на основе достаточно продолжительных обсуждений принята для публикации статья относительно применения в криптографии интегральных уравнений, как альтернативы алгебраическим методам. Надеемся, что по ней пройдут обсуждения и дискуссия в среде специалистов.

С наилучшими пожеланиями,

*профессор кафедры БИСТ
Харьковского национального
университета им. В.Н. Каразина,
Главный конструктор ПАТ «ИИТ»*



I.D. Gorbunov
И.Д. Горбунко

МЕТОДЫ СИНТЕЗА И АНАЛИЗА СИММЕТРИЧНЫХ ШИФРОВ

УДК 621.391:519.2

ШВИДКИЙ ІМОВІРНІСНИЙ АЛГОРИТМ ОЦІНЮВАННЯ ВІДСТАНІ МІЖ ЗРІВНОВАЖЕНОЮ БУЛЕВОЮ ФУНКЦІЄЮ ТА МНОЖИНОЮ k -ВИМІРНИХ ФУНКЦІЙ

С.М. КОНЮШОК, А.М. ОЛЕКСІЙЧУК, А.Ю. СТОРОЖУК

Запропоновано поліноміальний імовірнісний алгоритм обчислення значень нижніх меж відносної відстані між зрівноваженою булевою функцією від n змінних, що задається за допомогою оракула, та множиною k -вимірних функцій. Показано, що при малих значеннях k цей алгоритм може бути ефективно використано на практиці для аналізу кореляційних властивостей функцій ускладнення поточкових шифрів.

Ключові слова: нелінійний криптоаналіз, кореляційна атака, k -вимірна функція, ймовірнісний алгоритм, обґрунтування стійкості поточкових шифрів.

ВСТУП

Як відомо, необхідною умовою стійкості синхронних поточкових шифрів відносно кореляційних атак є неможливість наближення функцій ускладнення, що використовуються в їхніх конструкціях, більш просто збудованими функціями. Найвідомішими прикладами булевих функцій, які мають просту аналітичну будову, є афінні функції, а також функції, що залежать від малої кількості змінних. Більш широкий клас утворюють так звані k -вимірні функції, тобто булеві функції від довільної кількості n змінних, що є лінійно еквівалентними функціями від фіксованого числа $k < n$ змінних. Дослідженню властивостей таких функцій, зокрема, як можливих наближень довільних булевих функцій, присвячено роботи [1–7]. Відомі також різноманітні атаки на генератори гами поточкових шифрів, функції ускладнення яких є k -вимірними або близькими до таких [8–11].

Для обґрунтування стійкості поточкових шифрів відносно зазначених атак треба обчислювати або оцінювати знизу відстань між заданою булевою функцією та множиною всіх k -вимірних функцій від n змінних. Зауважимо, що ця задача є нетривіальною навіть при $k = 2$, якщо n є достатньо великим числом (наприклад, $n \geq 64$). Головна причина труднощів полягає в надвеликій кількості k -вимірних функцій від n змінних, перелічення яких у реальному часі (при зазначених n) є практично неможливим. Зменшити перебір дозволяють теореми 4 і 5 в [2] (або теорема 1 в [7]), проте і в цьому випадку алгоритм обчислення значення відстані між довільною булевою функцією та множиною k -вимірних функцій від n змінних вимагає, щонайменше, $2^{k(n-k)}$ операцій.

У даній статті пропонується ймовірнісний алгоритм обчислення значень нижніх меж шуканої відстані, складність якого залежить лінійно від n (та поліноміально від величин,

обернених до точності та ймовірності помилки алгоритму). Зазначений алгоритм базується на розвитку ідей робіт [12–15], остання з яких присвячена розв'язанню задачі оцінювання відстані в окремому випадку $k = 1$. Наведено результати моделювання запропонованого алгоритму, які дозволяють стверджувати про можливість його застосування на практиці під час дослідження кореляційних властивостей функцій ускладнення поточкових шифрів.

ПОСТАНОВКА ЗАДАЧІ ТА ОСНОВНІ ТЕОРЕТИЧНІ РЕЗУЛЬТАТИ

Нижче використовуються такі позначення:

V_n — векторний простір двійкових векторів довжини n ;

$V_n^* = V_n \setminus \{0\}$;

$F_{n \times k}$ — множина матриць розміру $n \times k$ над полем $F = \mathbf{GF}(2)$;

B_n — множина булевих функцій від n змінних;

$d(f, g) = 2^{-n} |\{x \in V_n : f(x) \neq g(x)\}|$ — відносна

відстань між функціями $f, g \in B_n$;

$d(f, U) = \min_{g \in U} d(f, g)$ — відносна відстань між

функцією $f \in B_n$ та множиною $U \subseteq B_n$;

$\hat{f}(\alpha) = 2^{-n} \sum_{x \in V_n} (-1)^{f(x) \oplus \alpha x}$, $\alpha \in V_n$ — нормовані

коефіцієнти Уолша-Адамара функції $f \in B_n$.

Функція $g \in B_n$ називається k -вимірною, якщо вона може бути подана у вигляді $g(x) = \varphi(xA)$, $x \in V_n$, де $\varphi \in B_k$, $A \in F_{n \times k}$, $k \in \{0, n-1\}$ [3, 4].

Позначимо $B_{n,k}$ множину всіх k -вимірних функцій від n змінних. На підставі теореми 1 в [7] відносна відстань між функцією $f \in B_n$ та множиною $B_{n,k}$ визначається за формулою

$$d(f, B_{n,k}) = 1/2 \cdot \left(1 - \max_{H \in L_{n,k}} I_f(H) \right), \quad (1)$$

де максимум береться за всіма k -вимірними підпросторами H векторного простору V_n ,

$$l_f(H) = 2^{-k} \sum_{s \in V_k} \left| \sum_{x \in H} \hat{f}(x)(-1)^{\alpha_s x} \right|, \quad (2)$$

а $\{\alpha_s : s \in V_k\}$ є системою представників усіх суміжних класів простору V_n по підпростору $H^\perp$, дуальному до H .

Припустимо, що f є зрівноваженою функцією, тобто задовольняє умову $\hat{f}(0) = 0$. Позначимо H^* довільний підпростір, на якому досягається максимум значень (2) у правій частині рівності (1) та зафіксуємо $n \times k$ -матрицю A , стовпці якої утворюють базис підпростору H^* . Тоді рівність (1) можна записати у вигляді

$$d(f, B_{n,k}) = 1/2 \cdot (1 - l_{f,A}), \quad (3)$$

де

$$l_{f,A} = 2^{-k} \sum_{s \in V_k} \left| \sum_{y \in V_k^*} \hat{f}(Ay)(-1)^{sy} \right|. \quad (4)$$

Припустимо зараз, що зрівноважена функція f задається за допомогою оракула, тобто певного алгоритму, що дозволяє обчислювати значення $f(x)$ для довільного вхідного набору $x \in V_n$. Треба розробити алгоритм, який обчислює для будь-яких $k \in \overline{1, n-1}$, $\varepsilon, \delta \in (0, 1)$ статистичну верхню оцінку параметра (4) з точністю ε та надійністю не менше $1 - \delta$, тобто таке випадкове значення $\theta \in (0, 1)$, що задовольняє умову

$$\mathbf{P}\{l_{f,A} \leq \theta + \varepsilon\} \geq 1 - \delta. \quad (5)$$

При цьому вимагається, щоб для будь-якого фіксованого k обчислювальна складність алгоритму поліноміально залежала від n , ε^{-1} та δ^{-1} .

Для викладення алгоритму, що пропонується, введемо низку позначень та доведемо одну теорему.

Зафіксуємо натуральне число $t > k$ та позначимо X випадкову матрицю з рівномірним розподілом ймовірностей на множині $F_{t \times n}$. Розглянемо випадкові величини

$$\xi_a(X) = \frac{1}{2^t - 1} \sum_{u \in V_t^*} (-1)^{f(uX) \oplus ua}, \quad a \in V_t, \quad (6)$$

$$\eta_B(X) = 2^{-k} \sum_{s \in V_k} \left| \sum_{y \in V_k^*} \xi_{By}(X)(-1)^{sy} \right|, \quad B \in F_{t \times k}. \quad (7)$$

Назвемо матрицю $B \in F_{t \times k}$ спеціальною ступеневою, якщо транспонована до неї матриця має вигляд

$$B^T = \begin{pmatrix} 0 \dots 0 & 1^* & \dots & 0^* & \dots & 0^* & \dots & * \\ 0 \dots 0 & 00 \dots 0 & 1^* & \dots & 0^* & \dots & * \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 \dots 0 & 00 \dots 0 & 00 \dots 0 & 1^* & \dots & * \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 \dots 0 & 00 \dots 0 & 00 \dots 0 & 00 \dots 0 & 1^* & \dots \end{pmatrix},$$

де $*$ означає довільний елемент поля F , $1 \leq i_1 < \dots < i_r \leq t$. Добре відомо (див., наприклад, [16], с. 149), що будь-яка матриця $B \in F_{t \times k}$ є стовпцево еквівалентною єдиній спеціальній ступеневій матриці, тобто існує точно одна зазначена матриця $\tilde{B}$, яка пов'язана з B співвідношенням $\tilde{B} = BU$, де U — оборотна матриця порядку k над полем F .

Позначимо $\tilde{F}_{t \times k}$ множину усіх спеціальних ступеневих матриць розміру $t \times k$ над F та покладемо

$$\theta(X) = \max_{B \in \tilde{F}_{t \times k}} \{\eta_B(X)\}. \quad (8)$$

Теорема 1. Нехай $k \in \overline{1, n-1}$, $\varepsilon, \delta \in (0, 1)$ і $2^t \geq 2^k \varepsilon^{-2} \delta^{-1}$. Тоді для випадкової величини $\theta = \theta(X)$ виконується нерівність (5).

Доведення. Перш за все, переконаємося у справедливості такої нерівності:

$$|l_{f,A} - \eta_{XA}(X)| \leq \left(\sum_{y \in V_k^*} (\hat{f}(Ay) - \xi_{XAy}(X))^2 \right)^{1/2}. \quad (9)$$

Дійсно, на підставі формул (4), (6) та нерівності між середнім арифметичним і середнім квадратичним

$$\begin{aligned} |l_{f,A} - \eta_{XA}(X)| &= \left| 2^{-k} \sum_{s \in V_k} \left(\sum_{y \in V_k^*} \hat{f}(Ay)(-1)^{sy} \right) - \sum_{y \in V_k^*} \xi_{XAy}(X)(-1)^{sy} \right| \leq \\ &\leq 2^{-k} \sum_{s \in V_k} \left| \sum_{y \in V_k^*} \left(\hat{f}(Ay) - \xi_{XAy}(X) \right)(-1)^{sy} \right| \leq \\ &\leq \left(2^{-k} \sum_{s \in V_k} \left(\sum_{y \in V_k^*} \left(\hat{f}(Ay) - \xi_{XAy}(X) \right)(-1)^{sy} \right)^2 \right)^{1/2}. \end{aligned} \quad (10)$$

Далі,

$$\begin{aligned} &2^{-k} \sum_{s \in V_k} \left(\sum_{y \in V_k^*} \left(\hat{f}(Ay) - \xi_{XAy}(X) \right)(-1)^{sy} \right)^2 = \\ &= 2^{-k} \sum_{y_1, y_2 \in V_k^*} \left(\hat{f}(Ay_1) - \xi_{XAy_1}(X) \right) \left(\hat{f}(Ay_2) - \xi_{XAy_2}(X) \right) \times \\ &\times \sum_{s \in V_k} (-1)^{s(y_1 \oplus y_2)} = \sum_{y \in V_k^*} \left(\hat{f}(Ay) - \xi_{XAy}(X) \right)^2. \end{aligned}$$

Підставляючи зазначений вираз у формулу (10), отримаємо нерівність (9).

Покажемо зараз, що

$$\mathbf{P}_X \{ |l_{f,A} - \eta_{XA}(X)| > \varepsilon \} \leq 2^{k-t} \varepsilon^{-2}. \quad (11)$$

Дійсно, на підставі формули (9) та нерівності Маркова справедливі такі оцінки:

$$\begin{aligned} &\mathbf{P}_X \{ |l_{f,A} - \eta_{XA}(X)| > \varepsilon \} \leq \\ &\leq \mathbf{P}_X \left\{ \sum_{y \in V_k^*} (\hat{f}(Ay) - \xi_{XAy}(X))^2 > \varepsilon^2 \right\} \leq \\ &\leq \varepsilon^{-2} \sum_{y \in V_k^*} \mathbf{E}(\hat{f}(Ay) - \xi_{XAy}(X))^2. \end{aligned} \quad (12)$$

Далі, безпосередньо з формули (6) випливає, що для будь-якого $y \in V_k^*$ математичне сподівання випадкової величини $\xi_{X_{Ay}}(X)$ дорівнює $\hat{f}(Ay)$. Отже,

$$\begin{aligned} & \sum_{y \in V_k^*} \mathbf{E}(\hat{f}(Ay) - \xi_{X_{Ay}}(X))^2 = \\ &= \sum_{y \in V_k^*} \mathbf{E}(\xi_{X_{Ay}}(X) - \mathbf{E}(\xi_{X_{Ay}}(X)))^2 = \sum_{y \in V_k^*} \mathbf{D}(\xi_{X_{Ay}}(X)) = \\ &= \frac{1}{(2^t - 1)^2} \sum_{y \in V_k^*} \mathbf{D} \left(\sum_{u \in V_t^*} (-1)^{f(uX) \oplus uX(Ay)} \right) = \\ &= \frac{1}{(2^t - 1)^2} \sum_{y \in V_k^*} \sum_{u \in V_t^*} \mathbf{D}((-1)^{f(uX) \oplus uX(Ay)}), \end{aligned}$$

де остання рівність випливає з того, що доданки в сумі під знаком дисперсії є попарно незалежними випадковими величинами. Нарешті, використовуючи тривіальну оцінку $\mathbf{D}((-1)^{f(uX) \oplus uX(Ay)}) \leq 1$, $u \in V_t^*$, $y \in V_k^*$, отримуємо, що

$$\sum_{y \in V_k^*} \mathbf{E}(\hat{f}(Ay) - \xi_{X_{Ay}}(X))^2 \leq \frac{2^k - 1}{2^t - 1} \leq 2^{k-t}.$$

Звідси на підставі формули (12) випливає нерівність (11).

Для завершення доведення залишається зауважити, що $\eta_B(X) = \eta_{BU}(X)$ для будь-яких матриці $B \in F_{t \times k}$ та оберненої матриці $U \in F_{k \times k}$. Отже, згідно з формулою (8), $\theta(X) \geq \eta_B(X)$ для довільної (а не тільки спеціальної ступеневої) матриці $B \in F_{t \times k}$. Зокрема, подія $\{I_{f,A} > \theta(X) + \varepsilon\}$ тягне подію $\{I_{f,A} > \eta_{XA}(X) + \varepsilon\}$, звідки на підставі нерівності (11) випливає, що

$$\begin{aligned} & P_X\{I_{f,A} > \theta(X) + \varepsilon\} \leq P_X\{I_{f,A} > \eta_{XA}(X) + \varepsilon\} \leq \\ & \leq P_X\{|I_{f,A} - \eta_{XA}(X)| > \varepsilon\} \leq 2^{k-t} \varepsilon^{-2}. \end{aligned}$$

Таким чином, за виконанням умови $2^t \geq 2^k \varepsilon^{-2} \delta^{-1}$ справедлива нерівність (5).

Теорему доведено.

Наведемо зараз ймовірнісний алгоритм обчислення нижніх меж параметра (3).

Вхід: зрівноважена функція $f \in B_n$, задана за допомогою оракула; числа $k \in \overline{1, n-1}$, $\varepsilon, \delta \in (0, 1)$.

1. Покласти

$$t = k + \lceil \log(\varepsilon^{-2} \delta^{-1}) \rceil, \quad (13)$$

згенерувати випадкову рівноймовірну булеву $t \times n$ -матрицю X та обчислити значення функції $f_X(u) = f(uX)$, $u \in V_t$.

2. Обчислити значення (6) за допомогою алгоритму швидкого перетворення Адамара.

3. Для кожної матриці $B \in \tilde{F}_{t \times k}$:

— за відомими значеннями (6) обчислити значення функції

$$h(y) = \begin{cases} \xi_{By}(X), & \text{якщо } y \in V_k^*; \\ 0, & \text{якщо } y = 0; \end{cases}$$

— обчислити значення

$$\hat{h}(s) = \sum_{y \in V_k^*} \xi_{By}(X) (-1)^{sy}, \quad s \in V_k$$

за допомогою алгоритму швидкого перетворення Адамара;

— покласти $\eta_B(X) = 2^{-k} \sum_{s \in V_k} |\hat{h}(s)|$.

4. Покласти $\theta(X) = \max_{B \in \tilde{F}_{t \times k}} \{\eta_B(X)\}$.

Результат: випадкове число

$$\Delta(f, B_{n,k}) = 1/2 \cdot (1 - (\theta(X) + \varepsilon)),$$

що задовольняє умову

$$P_X\{d(f, B_{n,k}) \geq \Delta(f, B_{n,k})\} \geq 1 - \delta.$$

Коректність алгоритму випливає з наведеної вище теореми.

Для оцінювання трудомісткості алгоритму доведемо допоміжне твердження.

Лема. Для будь-яких натуральних $k < t$ справедлива нерівність

$$|\tilde{F}_{t \times k}| \leq c(k+1) \max\{2^{k^2}, 2^{k(t-k)}\},$$

де $c^{-1} = \prod_{i=1}^{\infty} (1 - 2^{-i})$.

Доведення. З означення множини $\tilde{F}_{t \times k}$ випливає, що $|\tilde{F}_{t \times k}| = \sum_{i=0}^k \binom{t}{i}$, де

$$\binom{t}{i} = \frac{(2^t - 1)(2^{t-1} - 1) \dots (2^{t-i+1} - 1)}{(2^i - 1)(2^{i-1} - 1) \dots (2 - 1)}$$

є число i -вимірних підпросторів простору V_t , $i \in \overline{0, t}$. Використовуючи оцінку $\binom{t}{i} \leq c \cdot 2^{i(t-i)}$, $i \in \overline{0, t}$, отримуємо, що

$$|\tilde{F}_{t \times k}| = \sum_{i=0}^k \binom{t}{i} \leq c \sum_{i=0}^k 2^{i(t-i)} \leq c(k+1) 2^{t^2/4}.$$

Нехай $t \leq 2k$. Тоді в силу наведеної нерівності $|\tilde{F}_{t \times k}| \leq c(k+1) 2^{k^2}$. Якщо ж $t > 2k$, то

$$\binom{t}{i} \leq \binom{t}{k} \leq c \cdot 2^{k(t-k)}$$

для кожного $i \in \overline{0, k}$ і, отже, $|\tilde{F}_{t \times k}| \leq c(k+1) 2^{k(t-k)}$. Таким чином, у будь-якому випадку виконується нерівність

$$|\tilde{F}_{t \times k}| \leq c(k+1) \max\{2^{k^2}, 2^{k(t-k)}\},$$

що й треба було довести.

Теорема 2. Трудомісткість наведеного алгоритму в найгіршому випадку дорівнює

$$\begin{aligned} & T_{n,k}(\varepsilon, \delta) = \\ &= O\left(2^k (k + \varepsilon^{-2} \delta^{-1}) (n \varepsilon^{-2} \delta^{-1} + k^2 \max\{2^{k^2}, \varepsilon^{-2k} \delta^{-k}\})\right). \quad (14) \end{aligned}$$

Доведення. На кроці 1 потрібно виконати $O(2^t n)$ операцій (булевого додавання та звернення до функції f), а на кроці 2 — $O(2^t t)$ операцій (додавання та віднімання цілих чисел). Далі, для кожної фіксованої матриці $B \in \tilde{F}_{t \times k}$ на кроці 3 потрібно виконати $O(2^k t k)$ таких самих операцій. Отже, на підставі леми трудомісткість кроку 3 складає

$$O(2^k tk | \tilde{F}_{t \times k} |) = O(2^k tk^2 \max\{2^{k^2}, 2^{k(t-k)}\}).$$

Нарешті, трудомісткість четвертого кроку є $O(|\tilde{F}_{t \times k}|) = O(\max\{2^{k^2}, 2^{k(t-k)}\})$. Підсумовуючи отримані оцінки, з урахуванням рівності (13) отримуємо формулу (14).

Теорему доведено.

РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ ЗАПРОПОНОВАНОГО АЛГОРИТМУ

У табл. 1 показано чисельні значення двійкового логарифму виразу під знаком O у правій частині рівності (14). Як видно з таблиці, із збільшенням параметра k чи зменшенням параметра ϵ трудомісткість алгоритму досить швидко зростає. Навпаки, помітне збільшення параметра n практично не впливає на зростання трудомісткості алгоритму.

Таблиця 1

Чисельні оцінки трудомісткості алгоритму ($\delta = 0,0625$)

$\epsilon \backslash k$	2	3	4
1/2	20,3663	21,2143	22,7665
1/4	25,0112	25,5962	30,2263
1/8	30,3247	30,5878	38,1766
n	64	128	64

У табл. 2, 3 показано результати застосування запропонованого алгоритму при $k = 2$ до функцій від 64 та 11 змінних відповідно. Обчислення проводилися на ЕОМ з процесором Intel Core i7 (1,6 ГГц) та обсягом оперативної пам'яті 4 Гб RAM (DDR3) на базі Windows 7 (використовувався пакет прикладних програм Maple 13.0). Середній час роботи комп'ютерної програми складає 804,5 секунди при $n = 64$ та 652,1 секунди при $n = 11$.

У табл. 2 наведено значення

$$\Delta(f, B_{n,2}) = 1/2 \cdot (1 - (\theta(X) + \epsilon))$$

статистичних нижніх оцінок параметра $d(f, B_{n,2})$, отримані за допомогою запропонованого алгоритму для двох функцій вигляду

$$f(x) = f(x_1, x_2) = g(x_1, x_2)h_1(x_2) \oplus$$

$$(g(x_1, x_2) \oplus 1)h_2(x_2), \quad x = (x_1, x_2) \in V_{n_1} \times V_{n_2},$$

де $g(x_1, x_2) = (\alpha_1 x_1)(\alpha_2 x_2)$ — двовимірна функція, що не залежить суттєво від останніх n_2 змінних (α_1 та α_2 є різними ненульовими булевими векторами довжини n_1 , а $\alpha_i x_i$ означає булевий скалярний добуток векторів α_i та $x_i \in V_{n_1}$, $i = 1, 2$); h_1 та h_2 — довільні булеві функції від n_2 змінних, що задовольняють умову $wt(h_1) = 2^{-n_2}(2^{n_2+1} - 3m)$, $wt(h_2) = 2^{-n_2}m$, де m — ціле число таке, що $2^{n_2} < 3m < 2^{n_2+1}$. Як показує прямий підрахунок, у цьому випадку

$$\begin{aligned} wt(f) &= 1/4 \cdot wt(h_1) + 3/4 \cdot wt(h_2) = 1/2, \\ d(f, g) &= 1/4 \cdot (1 - wt(h_1)) + 3/4 \cdot wt(h_2) = \\ &= 1/4 + 1/2 \cdot (1 - wt(h_1)). \end{aligned}$$

Отже, f є зрівноваженою функцією від $n = n_1 + n_2$ змінних, що знаходиться від множини $B_{n,2}$ на відносній відстані не більше, ніж

$$\Delta^*(f, B_{n,2}) =$$

$$= \min\{1/4 + 1/2 \cdot (1 - wt(h_1)), 3/4 - 1/2 \cdot (1 - wt(h_1))\}. \quad (15)$$

Параметр m у таблиці задає функції h_1 та h_2 за правилом:

$$h_1(x_2) = 1 \Leftrightarrow |x_2| < 2^{n_2+1} - 3m,$$

$$h_2(x_2) = 0 \Leftrightarrow |x_2| < 2^{n_2} - m,$$

де $|x_2|$ — двійкове ціле число, що відповідає вектору $x_2 \in V_{n_2}$. Значення t і $\theta(X)$ обчислені, відповідно, на кроках 1 і 4 алгоритму, а в останній колонці таблиці показано значення параметра (15).

Таблиця 2

Статистичні нижні оцінки параметра $d(f, B_{n,2})$ ($n_1 = 20$, $n_2 = 44$, $\epsilon = 1/4$, $\delta = 0,0625$, $t = 10$)

Номер експерименту	m	$\theta(X)$	$\Delta(f, B_{n,2})$	$\Delta^*(f, B_{n,2})$
1	$(2^{44} + 5)/3$	0,5010	0,1245	0,25
2		0,5010	0,1245	
3		0,5191	0,1155	
4		0,5308	0,1096	
5	$(2^{45} - 5)/3$	0,5020	0,1240	0,25
6		0,5020	0,1240	
7		0,5059	0,1221	
8		0,5010	0,1245	
9		0,5020	0,1240	
10		0,5073	0,1213	

Табл. 3 демонструє результати застосування алгоритму до функції від 11 змінних, яка використовується в алгоритмі шифрування Achterbahn-128/80 [17]:

$$\begin{aligned} G(x_1, \dots, x_{11}) &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_9 \oplus x_{11} \oplus \\ &\oplus x_2 x_{10} \oplus x_2 x_{11} \oplus x_4 x_8 \oplus x_5 x_6 \oplus x_6 x_8 \oplus x_6 x_{10} \oplus x_6 x_{11} \oplus \\ &\oplus x_7 x_8 \oplus x_8 x_9 \oplus x_8 x_{10} \oplus x_9 x_{10} \oplus x_9 x_{11} \oplus x_1 x_2 x_8 \oplus \\ &\oplus x_1 x_4 x_{10} \oplus x_1 x_4 x_{11} \oplus x_1 x_8 x_9 \oplus x_1 x_9 x_{10} \oplus x_1 x_9 x_{11} \oplus \\ &\oplus x_2 x_3 x_8 \oplus x_2 x_4 x_8 \oplus x_2 x_4 x_{10} \oplus x_2 x_4 x_{11} \oplus x_2 x_7 x_8 \oplus \\ &\oplus x_2 x_8 x_{10} \oplus x_2 x_8 x_{11} \oplus x_2 x_9 x_{10} \oplus x_2 x_9 x_{11} \oplus x_3 x_4 x_8 \oplus \\ &\oplus x_3 x_8 x_9 \oplus x_4 x_7 x_8 \oplus x_4 x_8 x_9 \oplus x_5 x_6 x_8 \oplus x_5 x_6 x_{10} \oplus \\ &\oplus x_5 x_6 x_{11} \oplus x_6 x_8 x_{10} \oplus x_6 x_8 x_{11} \oplus x_7 x_8 x_9 \oplus x_8 x_9 x_{10} \oplus \\ &\oplus x_8 x_9 x_{11} \oplus x_1 x_2 x_3 x_8 \oplus x_1 x_2 x_7 x_8 \oplus x_1 x_3 x_5 x_8 \oplus x_1 x_3 x_8 x_9 \oplus \\ &\oplus x_1 x_4 x_8 x_{10} \oplus x_1 x_4 x_8 x_{11} \oplus x_1 x_5 x_7 x_8 \oplus x_1 x_7 x_8 x_9 \oplus x_1 x_8 x_9 x_{10} \oplus \\ &\oplus x_1 x_8 x_9 x_{11} \oplus x_2 x_3 x_4 x_8 \oplus x_2 x_3 x_5 x_8 \oplus x_2 x_4 x_7 x_8 \oplus x_2 x_4 x_8 x_{10} \oplus \\ &\oplus x_2 x_4 x_8 x_{11} \oplus x_2 x_5 x_7 x_8 \oplus x_2 x_8 x_9 x_{10} \oplus x_2 x_8 x_9 x_{11} \oplus x_3 x_4 x_8 x_9 \oplus \\ &\oplus x_4 x_7 x_8 x_9 \oplus x_5 x_6 x_8 x_{10} \oplus x_5 x_6 x_8 x_{11}, \quad (x_1, \dots, x_{11}) \in V_{11}. \end{aligned}$$

Обчислення відносної відстані $d(G, B_{n,2})$ за формулою (1) показує, що її точне значення дорівнює 0,4375. При цьому час обчислення складає 3020 секунд, що приблизно в 5 разів переви-

щує середній час оцінювання цього параметра з точністю $\varepsilon = 1/8$ та надійністю $1 - \delta \geq 0,75$ (див. табл. 3).

Таблиця 3

Статистичні нижні оцінки параметра $d(G, B_{n,2})$
($n = 11$, $\varepsilon = 1/8$, $\delta = 0,25$, $t = 10$)

Номер експерименту	$\theta(X)$	$\varphi(G, B_{n,2})$
1	0,2517	0,3316
2	0,1881	0,3434
3	0,1881	0,3434
4	0,1266	0,3742
5	0,1881	0,3434
6	0,2512	0,3119
7	0,2498	0,3126
8	0,1891	0,3429
9	0,1891	0,3429
10	0,2507	0,3121

Для підвищення точності оцінок, наведених у табл. 2 і табл. 3, слід зменшити значення ε , що призведе до збільшення часу виконання алгоритму. Наприклад, при $\varepsilon = 1/8$ нижня оцінка параметра $d(f, B_{n,2})$ становить приблизно 0,1871, при цьому середній час роботи комп'ютерної програми складає майже 4 години.

В цілому, отримані результати показують, що при малих значеннях k запропонований алгоритм може бути ефективно використано на практиці для аналізу кореляційних властивостей функцій ускладнення поточкових шифрів.

Література

- [1] Dawson E. Construction of correlation immune Boolean functions / E. Dawson, C.K. Wu // Information and Communication Security, Proceedings. Berlin. Springer-Verlag. 1997. — P. 170–180.
- [2] Canteaut A. On the correlations between a combining function and function of fewer variables / A. Canteaut // The 2002 IEEE Information Theory Workshop, Proceedings. Berlin. Springer-Verlag. 2002. — P. 78–81.
- [3] Gopalan P. A Fourier-analytic approach to Reed-Muller decoding / P. Gopalan // Annual IEEE Symp. on Foundation in Computer Science. — FOCS 2010, Proceedings. Berlin. Springer-Verlag. 2010. — P. 685–694.
- [4] Gopalan P. Testing Fourier dimensionality and sparsity / P. Gopalan, R. O'Donnell, A. Servedio, A. Shpilka, K. Wimmer // SIAM J. on Computing. 2011. V. 40(4). — P. 1075–1100.
- [5] Алексеев Е. К. О некоторых мерах нелинейности булевых функций / Е. К. Алексеев // Прикладная дискретная математика. 2011. № 2(12). — С. 5–16.
- [6] Алексейчук А. Н. Усовершенствованный тест k-мерности для булевых функций / А. Н. Алексейчук, С. Н. Конюшок // Кибернетика и системный анализ. 2013. Т. 49. № 2. — С. 27–35.
- [7] Алексейчук А. Н. Алгебраически вырожденные приближения булевых функций / А. Н. Алексейчук, С. Н. Конюшок // Кибернетика и системный анализ. 2014. Вып. 50. № 5 (в печати).
- [8] Daemen J. Resynchronization weaknesses in synchronous stream ciphers / J. Daemen, R. Govaerts, J. Vandewalle // Advances in Cryptology. — EURO-CRYPT'93, Proceedings. Berlin. Springer-Verlag, 1993. — P. 159–167.
- [9] Golić J. On the resynchronization attack / J. Golić, G. Morgari // Fast Software Encryption. — FSE'03, Proceedings. Berlin. Springer-Verlag, 2003. — P. 100–110.
- [10] Алексеев Е. К. Об атаке на фильтрующий генератор с функцией усложнения, близкой к алгебраически вырожденной / Е. К. Алексеев // Сборник статей молодых ученых факультета МВК МГУ, 2011. — Вып. 8. — С. 114–123.
- [11] Алексейчук А. Н. Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной / А. Н. Алексейчук, С. Н. Конюшок, А. Ю. Сторожук // Прикладная радиоэлектроника. 2014. — Вып. 176. — С. 13–21.
- [12] Levin L.A. Randomness and non-determinism / L.A. Levin // J. of Symbolic Logic. 1993. Vol. 58. № 3. — P. 1102–1103.
- [13] Bshouty N. More efficient PAC-learning of DNF with membership queries under the uniform distribution / N. Bshouty, J. Jackson, C. Tamon // Proc. 12th Annual Conf. on Comput. Learning Theory, 1999. — P. 286–295.
- [14] Алексейчук А. Н. Быстрый алгоритм статистического оценивания максимальной несбалансированности билинейных аппроксимаций булевых отображений / А. Н. Алексейчук, А. С. Шевцов // Прикладная дискретная математика. 2011. — № 3(13). — С. 5–11.
- [15] Алексейчук А. Н. О статистических свойствах нелинейности сужений булевых функций на случайно выбранное подпространство / А. Н. Алексейчук, С. Н. Конюшок // Прикладная дискретная математика. 2012. — Вып. 1(15). — С. 5–10.
- [16] Глухов М. М. Алгебра / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. — Учеб. в 2-х т., Т. 1. — М.: Гелиос АРВ, 2003. — 336 с.
- [17] Gammel B. M. Achterbahn-128/80 / B. M. Gammel, R. Gottfert, O. Kniffner // eSTREAM, ECRYPT Stream Cipher Project, Report 2006/001, 2006.

Надійшла до редколегії 4.06.2014



Конюшок Сергій Миколайович, кандидат технічних наук, доцент, заступник (з навчальної та наукової роботи) начальника Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ". Галузь наукових інтересів: криптографічні властивості булевих функцій.



Олексійчук Антон Миколайович, доктор технічних наук, доцент, професор кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ". Галузь наукових інтересів: теоретична криптографія.



Сторожук Артем Юрійович, аспірант Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ". Галузь наукових інтересів: прикладна криптографія.

УДК 621.391:519.2

Быстрый вероятностный алгоритм оценивания расстояния между уравновешенной булевой функцией и множеством k -мерных функций / С.М. Конюшок, А.Н. Алексейчук, А.Ю. Сторожук // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 186–191.

Предложен полиномиальный вероятностный алгоритм вычисления значений нижних границ относительного расстояния между уравновешенной булевой функцией от n переменных, заданной с помощью оракула, и множеством k -мерных функций. Показано, что при малых значениях k этот алгоритм может быть эффективно использован на практике для анализа корреляционных свойств функций усложнения поточных шифров.

Ключевые слова: нелинейный криптоанализ, корреляционная атака, k -мерная функция, вероятностный алгоритм, обоснование стойкости поточных шифров.

Табл.: 3. Библиогр.: 17 назв.

UDC 621.391:519.2

Fast probabilistic algorithm for distance evaluation between balanced Boolean function and set of k -dimensional functions / S.N. Konyushok, A.N. Alekseychuk, A.Yu. Storozhuk // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 186–191.

A polynomial probabilistic algorithm for computing the values of lower bounds of the relative distance between a balanced Boolean function in n -variables (defined by an oracle) and a set of k -dimensional functions is proposed. It is shown that for small values of k this algorithm can be efficiently used in practice to analyze the correlation properties of Boolean functions used in stream ciphers.

Keywords: non-linear cryptanalysis, correlation attack, k -dimensional function, probabilistic algorithm, stream ciphers resistance proof.

Tab.: 3. Ref.: 17 items.

RELATED-KEY CRYPTANALYSIS OF PERSPECTIVE SYMMETRIC BLOCK CIPHER

ROMAN OLIYNYKOV, DMYTRO KAIDALOV

Symmetric block ciphers are among the most widely used cryptographic primitives. In addition to providing privacy via encryption, block ciphers are used as basic components in the construction of hash functions, message authentication codes, pseudorandom number generators as part of various cryptographic protocols etc. One of the most popular block ciphers nowadays is AES (Advanced Encryption Standard), which is used as a standard of symmetric encryption in many countries of the world. Several years ago a theoretical attack against the AES key-expansion algorithm was suggested, and complexity of this attack turned out to be significantly lower compared to brute force search. This paper considers the method of estimating encryption algorithm security against related-key attacks, and its application to the perspective block cipher, which is a candidate to the block encryption standard in Ukraine.

Keywords: block cipher, cryptanalysis, related key attack.

1. INTRODUCTION

From [5,6,7] it is known that related-key attacks were found for algorithms AES-192 and AES-256 which significantly reduced the theoretical security level of these algorithms. That is why the question about new SPN-based block cipher which would be secure from attacks which is present in AES is arisen.

In this article a new improved SPN-like cipher is presented and its security estimation is made. Authors propose this cipher as a perspective algorithm [4,17] which is based on the AES but has significant improvements such as a new key expansion scheme, resistance against algebraic attacks, higher productivity, etc. The new encryption algorithm was proposed to the public competition of block cipher selection to be a prototype during development of Ukrainian National Standard [4,17]. That is the main reason of researching this cipher.

But the security proof against related-key attacks is highly required. This is a challenging problem to solve since for now there are not so many efficient algorithms for estimating cipher security against related-key attacks. So the main goal of our research was to develop such algorithm. The article contains detailed description of developed algorithm, its complexity and result of applying this algorithm to the described SPN-based cipher.

2. RELATED-KEY ATTACK FOR MODERN BLOCK CIPHERS

2.1 Description of related-key attack for AES

Brief description of this attack is taken from [5]. This attack is based on the differential cryptanalysis [16]. The idea of this attack is to inject a difference into the internal state, causing a disturbance, and then to correct it with the next injections. The resulting difference pattern is spread out due to the message schedule causing more disturbances in other rounds. The goal is to have as few disturbances as possible in order to reduce the complexity of the attack [5].

In the related-key scenario it is allowed to inject difference into the key, and not only into the plain-

text as in the pure differential cryptanalysis. However the attacker cannot control the key itself and thus the attack should work for any key pair with a given difference.

Local collisions in AES-256 are best understood on a one-round example (fig. 1).

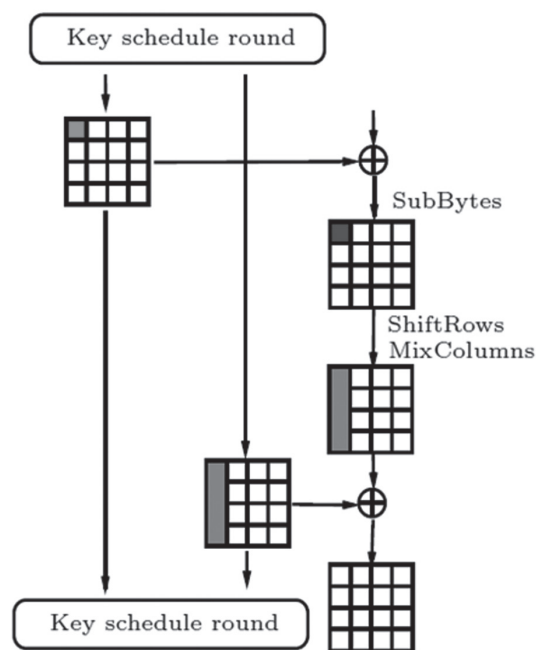


Fig. 1. Local collisions in AES[5]

Here one active S-box is needed (it is a short name for bytes Substitution operation) and five non-zero byte differences in the two subkeys. These five bytes split into two parts: one-byte disturbance and four-byte correction.

Due to the key schedule the differences spread to other rounds. Most of the AES key schedule operations are linear, so a sequence of several consecutive round key values can be viewed as a codeword of a linear code. This is the case, particularly, when a trail does not have active S-boxes in the key schedule.

Let figure out how to build an optimal trail for the key recovery attack. Typically, a trail is better if it has fewer active S-boxes. Disturbance differences

form a codeword, which should have low weight. Simultaneously, correction differences also must form a codeword, and the key schedule codeword is the sum of the disturbance and the correction codewords. In further trails, the correction codeword is constructed from the former one by just shifting four columns to the right and applying the S-box and Mix Columns expansion. Synchronization is simple since the injection is made to the first row, which is not rotated by Shift Rows. Otherwise, the task of synchronizing two codewords would have been much harder and would have lead to high-weight codewords [5].

An example of a good key-schedule pattern for AES-256 is depicted in fig. 2 as a 4.5-round codeword.

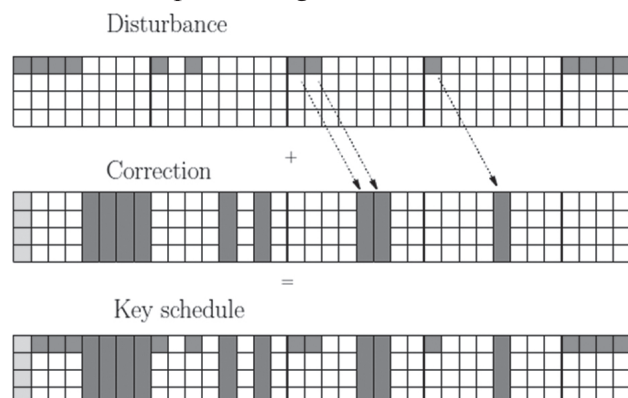


Fig. 2. AES-256 key schedule codeword (4.5 key-schedule rounds)[5]

In the first four key-schedule rounds the disturbance codeword has only 9 active bytes, which is the lower bound. It is needed to avoid active S-boxes in the key schedule as long as possible. Due to a weak diffusion in the AES key schedule the difference affects only one more byte per key schedule round. The correction column should be positioned four columns to the right, and propagates backwards in the same way. The last column in the first round key is active, so all S-boxes of the first round are active as well, which causes unknown difference in the first column. This «alien» difference should be canceled by the plaintext [5].

So such collisions can considerably reduce the complexity of key-recovery attack.

2.2 Current researches on the automatic search for related-key differential characteristics

Automatic search for best differential characteristics was first performed by Matsui [12] for DES. Algorithms for automatic search of differential characteristics for MD4 were presented in [13], and for MD5 in [14]. De Canni_ere and Rechberger in [15] described a method that finds characteristics in SHA-1 in an automatic way.

The first automatic tool for finding related-key differential characteristics was presented by Alex Biryukov and Ivica Nikolic in [11]. They described algorithm which allows to compute differential characteristics for AES, Camellia, Khazad and others. General idea of our searching algorithm is close to the one in [11]. But unlike algorithm from Biryukov

and Nikolic which controls each byte of state, in the presented algorithm entire column is controlled for amount of active bytes in it without exact position of these bytes. It is become possible because of the structure of researched encryption algorithm. Such scheme decreases the complexity of computation and reduces influence of high branching mentioned in [11].

3. PERSPECTIVE SPN-BASED BLOCK CIPHER

This section describes all parts of proposed SPN cipher in details because our estimation algorithm is based on it. As was mentioned before this cipher is based on the AES. The main differences compared to AES are the following: pre- and post-whitening using modulo addition, expanded size of MDS matrix for linear transformation, application of several S-boxes optimized with respect to differential, linear and algebraic cryptanalysis, and considerably redesigned key expansion procedure.

3.1 General parameters

This algorithm can be used with different types of input data. The block of input data can be 128, 256 or 512 bits. The length of the key can be also 128, 256 or 512 bits [4, 17].

The state of the cipher can be represented as a matrix. Each element of the matrix is a byte. Matrix consists of N_b columns. Each column consists of 8 bytes. So in total matrix has $8 * N_b$ bytes.

In the next table (table 1) acceptable combinations of different blocks and keys are represented.

Table 1

Acceptable combinations of blocks and keys

Size of block, bits	Supported key size, bits
128 ($N_b = 2$)	128, 256
256 ($N_b = 4$)	256, 512
512 ($N_b = 8$)	512

Amount of encryption rounds depends on the size of block and key. Amount of rounds for different versions of cipher is represented in the table 2.

Table 2

Amount of encryption rounds for different versions of cipher

Size of block, bits	Size of key 128 bits	Size of key 256 bits	Size of key 512 bits
128 ($N_b = 2$)	10	14	-
256 ($N_b = 4$)	-	14	18
512 ($N_b = 8$)	-	-	18

The research deals with the 128-bits version of the cipher, so in the next chapters presented information concerns only this version, even if it is not evidently mentioned.

3.2 Basic transformations

In the presented algorithm four basic transformations are used:

- key addition;
- bytes substitution;

- shift rows;
- mix columns.

These transformations are the base of all high-level structure [4, 17].

3.3 Key expansion scheme

Let K_M be the main key of encryption and $(K_1, K_2, \dots, K_m)$ are the round keys which are generated by key expansion scheme.

The cipher has an SPN structure which is based on the AES cipher:

$$Cipher_{K_M} = \prod_{i=1}^{N_r} \theta \circ \gamma \circ \sigma_{K_i}$$

Symbols: σ_{K_i} – round key adding; γ – nonlinear layer (bytes substitution); θ – linear layer (mix columns, shift rows); N_r – amount of rounds in block cipher.

Proposed key-expansion scheme contains two steps:

1. Computing of intermediate value κ_i which is based on the master key of encryption K_M and some constant.
2. Computing of round keys $(K_1, K_2, \dots, K_m)$ which are based on the master key K_M , intermediate value κ_i and some constant.

Intermediate value κ_i is computed with the next algorithm (fig. 3):

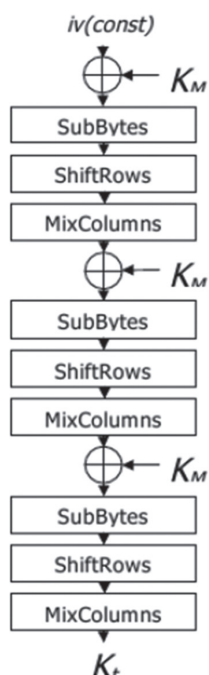


Fig. 3. Computing of intermediate value κ_i

As it is shown in figure 3 this algorithm contains all those transformations which are used in the cipher. This reduces implementation complexity because all basic operations are the same.

Computing of intermediate value can be formalized with the following formulas:

$$IM_{K_M} = \prod_{i=1}^3 \theta \circ \gamma \circ \sigma_{K_M}$$

$$K_i = IM_{K_M}(iv)$$

where iv is some constant which reduces symmetry in the key.

Generation of round keys can be formalized with next expression:

$$RK_{K_i}[K_M] = \sigma_{K_i + tmv_0} \circ \prod_{i=1}^2 \theta \circ \gamma \circ \sigma_{K_i + tmv_i}$$

where tmv_i are constants which are used for generation round keys. For each round this value should be unique but computation of these constants can be very simple (for example it is a simple shift on a few positions).

General algorithm for round keys generation is represented on the figure 4 [4, 17].

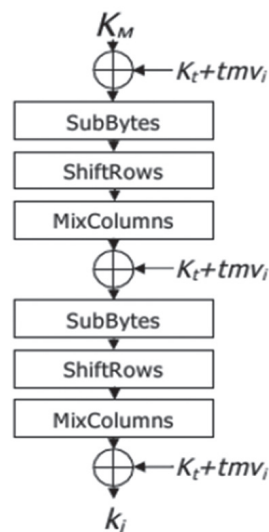


Fig. 4. Computation of round keys

The above scheme (figure 4) is similar to the scheme of computation κ_i and also it is similar to the general scheme of the cipher. This issue reduces the complexity of implementation.

According to the [10] such scheme of key expansion has some properties, such as:

1. One-way mapping: having encryption key it is very easy to generate round keys, but having one or more round keys it is computationally very difficult to retrieve encryption key or another round key.
2. Non-linear dependence between each bit of encryption key.
3. Good statistical properties of this key schedule (verified by NIST STS statistical tests).
4. Simple implementation (based on cipher round transformations only), good key agility and possibility to generate round keys in direct and reverse order with the same computational complexity.

3.4 Encryption transformation

Encryption transformation is almost the same as in AES algorithm. General scheme for 128-bits version of cipher is represented in figure 5. Adding keys K_0 and K_{10} are performed by modulo 2^{64} . In other cases simple XOR operation is used [4, 17].

As it has seen this cipher is a classic SPN structure. The same structure is used in key-expansion algorithm so it simplifies implementation.

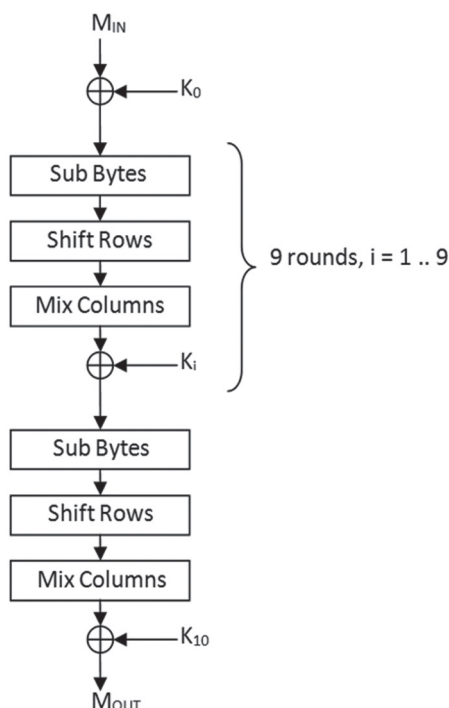


Fig. 5. Main encryption loop for 128 bit block and key cipher

4. THE ALGORITHM FOR ESTIMATION CIPHER SECURITY AGAINST RELATED-KEY ATTACKS

4.1 Proposed method for cipher security estimation

To prove the security of encryption algorithm against such type of attacks it is needed to find the best differential characteristic. The best characteristic is such one that has as few active bytes as possible. So after the best differential characteristic is found the amount of active bytes which were used during its construction should be counted. Active byte is a non-null byte which was passed through the substitution table. As it is known substitution of bytes is a non-linear transformation so the output is undefined and attacker should attack each active substitution transformation (which has complexity of 2^6 operations). If the amount of active bytes exceeds some boundary value the cipher can be considered as safe against key-related attacks because the complexity becomes bigger than the complexity of brute force attack on the cipher. Boundary value depends on the size of cipher block and size of encryption key.

The best differential characteristic can be found by searching between all possible input differences. This can be done automatically with special software. As it is shown later this search can be done in reasonable time for 128-bits version of cipher. To do this a special technique should be used. It is shown in the next chapters.

4.2 The algorithm for counting active bytes

As was mentioned before the best differential characteristic (with the fewest amounts of active bytes) can be found by searching between all possible input differences. For each characteristic the amount

of active bytes after key-expansion scheme and after all rounds of encryption should be counted. Proposed algorithm is for 128-bits version of the cipher.

Let examine the next example. It is a differential characteristic for Kt -computation. As was mentioned before Kt is an intermediate value which is computed in the key-expansion scheme. General scheme for computation of Kt is represented in figure 6.

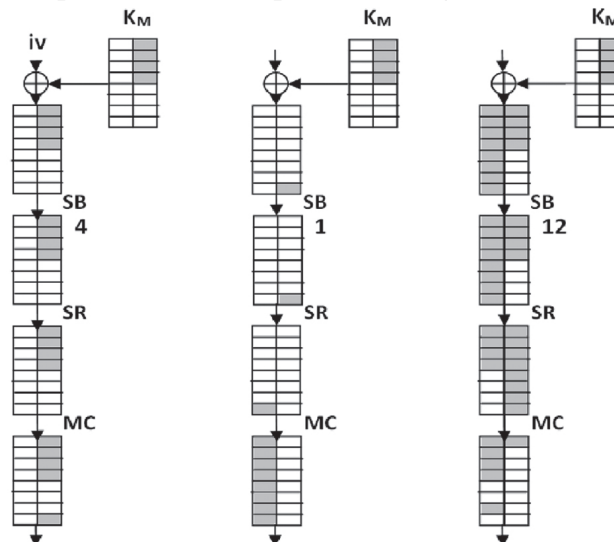


Fig. 6. Differential characteristic for Kt computation

Symbols: iv – the difference in initial vectors (always equals zero); K_M – master key of encryption (which is needed to be expanded); SB – sub-bytes (bytes substitution with substitution tables); SR – shift rows; MC – mix columns.

In the example (Figure 6), three rounds (from left to right) of Kt computation are shown. Input data is a difference of encryption key K_M . Then it is checked how this difference spreads after different transformations. Interested data is the amount of active bytes (such bytes for which difference is not null) on the input of Sub-Bytes transformation. In the example this value equals to 4 for the first round, 1 for the second round and 12 for the third round. In general there are 17 active bytes.

It should be mentioned that in other transformations (which is linear) the decision is based on what is the best for cryptanalyst. For example the difference after Mix Columns has such value that when it is added to the key K_M in the second round collision is occurred.

4.2.1 General description. Simpler algorithm for counting active bytes can be implemented. In this case each column of the state is controlled instead of each byte. It is known that the state of the cipher is represented as columns. Each column consists of 8 bytes. Thus 128-bits version has two columns. In the searching algorithm the amount of active bytes in columns is counted without their exact position. Such algorithm considerably reduces complexity. Accuracy of the results becomes worse because it is possible to find characteristic which does not really exist. Such characteristics are cutting down the acceptable boundary of amount of active bytes.

Thus may be said that a minimal amount of active bytes which is possible to achieve with any differential characteristic was found. This is a very good result.

If the amount of active bytes for investigated algorithm does not exceed theoretical boundary then such cipher is safe against the related-key attacks.

Figure 7 presents an example of differential characteristic for Kt -computation scheme. As shown in example the amount of active bytes after each transformation is recalculated. The numbers in figure are amounts of active bytes in columns. This example gives 3 active bytes in each round and 9 active bytes in total.

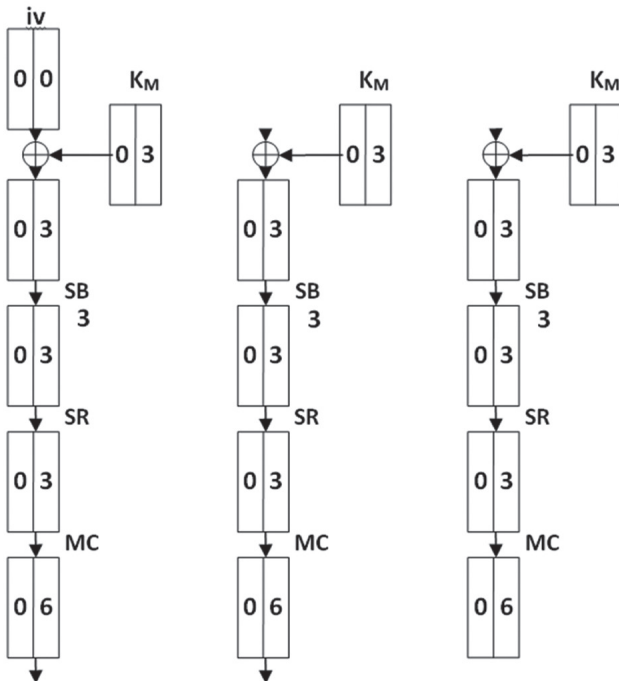


Fig. 7. Computation of active bytes

In order to make it more understandable in the next sections each transformation is described in details.

4.2.2 Key addition. The operation of adding with key is performed with the next rule: the value of one column is substituted from the value of corresponding column from key state. Then an absolute value of this result is taken. Some examples are represented in figure 8.

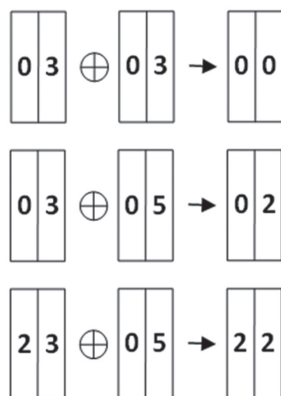


Fig. 8. Key addition

During adding it is assumed that non-zero bytes have such positions and values that collisions is occur. It means that it is the best case for the cryptanalyst. That is why this assumption can lower the resulting amount of active bytes but cannot increase it.

4.2.3 Bytes substitution. During bytes substitution transformation the amount of non-zero bytes does not change. That is why the values in the columns are not changed. But this transformation is very important because the security of the cipher depends on amount of non-zero bytes which are passed through the substitution tables. Such bytes become active bytes. The more active bytes the better cipher.

4.2.4 Shift rows. The operation of shifting bytes in 128-bits version of the cipher is performed as in figure 9:

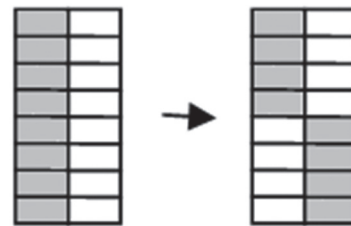


Fig. 9. Shift rows

Figure 9 shows that last 4 bytes of left and right columns change places. In algorithm only amount of non-zero bytes in column is controlled but the actual places of these bytes are undefined. Challenging problem here is how the shift should be performed and what amount of bytes should be shifted from one column to another. This problem was solved in such way: all possible variants of shifting were taking into account so the differential characteristic can get additional branches which are independent between each other. This part is the hardest part in the algorithm. It takes a lot of computation because on each round new branches appear and amount of these independent branches is growing exponentially depends on the amount of rounds.

Example of this transformation is represented in figure 10.

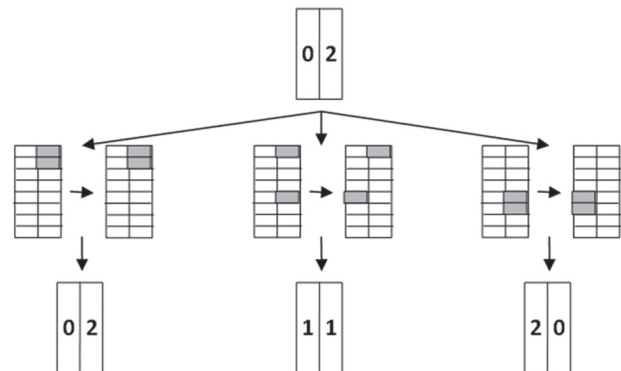


Fig. 10. Shift rows

Above example (Figure 10) shows that the state (0; 2) has three independent branches for continuation and for finding best differential characteristic, all this branches should be computed.

Table 3 represents amount of different alternatives for shifting in the column depends on amount of non-zero bytes.

Table 3

Amount of branches depends on amount of non-zero bytes in column

Amount of non-zero bytes in column	Amount of branches
0	1
1	2
2	3
3	4
4	5
5	4
6	3
7	2
8	1

Total amount of branches after shift rows transformation is equal to the product of possible shifts of the left and right columns. For example if left column has 3 non-zero bytes and right column has 4 non-zero bytes then the amount of branches for this transformation is $4 \cdot 5 = 20$.

4.2.5 Mix columns. Mixing in columns is performed as the product of column and some fixed matrix. The main property of this transformation is a fact that the sum of non-zero bytes on the input and output cannot be less than 9:

$$N_{in} + N_{out} \geq 9.$$

Exception is the situation when column has no active bytes, then on the output there is also no active bytes.

In the developed algorithm it is assumed that the best case for the cryptanalyst is taken. It means that there is always 9:

$$N_{in} + N_{out} = 9.$$

Some examples of how Mix Columns works are represented in figure 11.



Fig. 11. Mix columns

This transformation does not create new branches.

4.3 Description of results

The minimal safe threshold for estimated cipher is 26 active bytes. This value is derived from the next equation:

$$(2^{-5})^x < 2^{-128},$$

where 2^{-128} – probability of breaking the cipher with brute force attack; 2^{-5} – probability of breaking one substitution box of perspective cipher with brute force attack.

So if there are 26 active bytes it means that the entire complexity of breaking the cipher with such differential characteristic is 2^{-130} which is more than

the complexity of brute force attack. 25 active bytes gives the complexity less than 2^{-128} . So the minimal safe threshold is 26 active bytes.

As a result of experiments the best differential characteristic for 128-bits version of cipher was found. This characteristic has 27 active bytes. The results for each round are represented in the table 4.

Table 4

Description of best differential characteristic

Part of cipher	Round	Amount of active bytes	Accumulated amount of active bytes
Kt computation	1	7	7
	2	4	11
	3	2	13
Key expansion scheme	1	2	15
	2	2	17
Main encryption loop	1	1	18
	2	1	19
	3	1	20
	4	1	21
	5	1	22
	6	1	23
	7	1	24
	8	1	25
	9	1	26
	10	1	27
TOTAL			27

Table 4 shows that the differential characteristic in the main encryption loop is iterative and 1 active byte is added on each round. Detailed characteristic is represented in the next figures.

Symbols: K – round key. For different stages of cipher this value is different; SR – Shift Rows; MC – Mix Columns.

The stage of computing Kt is represented in figure 12. In this figure first 3 rounds are represented. As was mentioned before intermediate value Kt is needed for key expansion scheme.

Initially the state of transformation is equal to (0;0) and key is equal to (1;6). This key is the master key which is chosen. To be more precisely these values are the differences between keys or states.

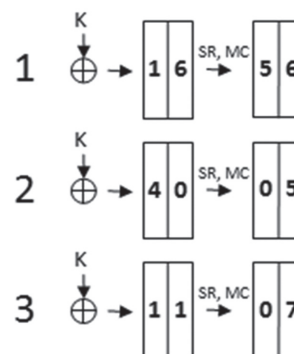


Fig. 12. Kt computation

In figure 13 two round of key-expansion scheme are represented. Initially the state of transformation is

equal to (0;7). This value is output value of previous transformation. The difference of the key is equal to (1;6). This is the master key.

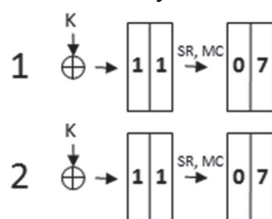


Fig. 13. Round key computation

In figure 14 ten rounds of the main encryption loop are represented. On this stage input states can be chosen so in this differential characteristic the input state (0;6) is taken. Round key is equal to (0;7). This is the output value of previous stage. The difference (0;7) is the same for all round keys because all of them have the same difference. So the values on each round also are equal

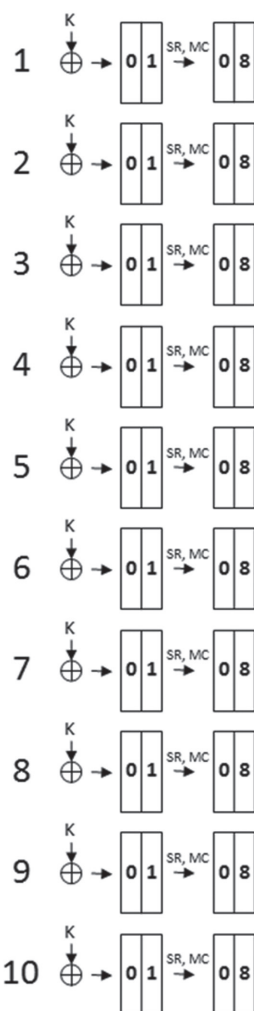


Fig. 14. Main encryption loop

The result is a differential characteristic which has 27 active bytes for 128-bits version of cipher. The theoretical threshold value for this version of cipher is equal to 26 active bytes. But as was mentioned before the obtained value is the minimum amount of active bytes which can be achieved. Practically the amount of active bytes in best differential characteristic can be

higher but it cannot be lower. This is the main property of algorithm. This issue is connected with the implementation of algorithm. This implementation allows to find characteristics which are impossible in practice. But still this algorithm can show the security of investigated cipher. For example if the amount of active bytes is lower than the threshold it is possible to find differential characteristic with such amount of active bytes which is potentially can lead to vulnerabilities.

4.4 Complexity of algorithm

The input values of algorithm are the different values of differences of the master key on the input of key-expansion scheme (it is a stage of Kt computation). The algorithm was build in such way that it controls 2 columns. Each column can have values between 0 to 9 (amount of active bytes). This means that each column have 9 different variants of input values. 128-bits version of cipher has 2 columns. The values of each column can be picked independently so the total amount of input values is 81 (formula 5).

$$N_{MK} = N_{Col}^c = 9^2 = 81 \quad (1)$$

Symbols: N_{MK} – amount of differences for master key; N_{Col} – amount of states for one column; c – amount of columns in the cipher state.

Also different open texts can be chosen on the input of main loop of encryption. Amount of different open texts are the same as amount of keys. It can be calculated with the next formula:

$$N_{PT} = N_{Col}^c = 9^2 = 81 \quad (2)$$

N_{PT} – amount of possible differences for open texts.

Also as mentioned before the Shift Rows transformation can create new branches. It means that additional paths for searching differential characteristic appear. It is connected with different possibilities of shifts. Algorithm does not control each byte separately but it controls amount of active bytes in columns. That is why different variants of shifts appear because the positions on which the active bytes are placed are unknown. Amount of such variants depends on amount of active bytes in column. Table 5 represents amount of branches which are created after Shift Rows for one column.

Table 5

Amount of branches depends on the amount of active bytes in column

Amount of active bytes in column	Amount of branches
0	1
1	2
2	3
3	4
4	5
5	4
6	3
7	2
8	1

To find total amount of branches after Shift Rows transformation it is needed to multiply amount of branches for each column.

$$N_{DC} = \prod_{i=0}^c N_i \quad (3)$$

N_{DC} – amount of branches after Shift Rows transformation; c – amount of columns in the cipher state; N_i – amount of branches for each column (according to table 3).

For example if current state of cipher is (3;4) then after Shift Rows there are $4 \cdot 5 = 20$ independent branches for searching differential characteristic.

The algorithm is searching among all possible input text differences. Each column on the average makes 3 different branches. It means that there are 9 different branches for the whole transformation for 128-bits version of cipher.

This transformation is the most complex one because it is performed in each round so there is an exponential growth of complexity. Formula 4 demonstrates amount of branches depends on the amount of rounds.

$$N_{DC} = \prod_{i=0}^r \prod_{j=0}^c N_{ij} \quad (4)$$

N_{DC} – total amount of branches; c – amount of columns in the cipher state; r – amount of rounds; N_{ij} – amount of branches for each column for one round (according to table 5).

The complexity of algorithm can be reduced with filtering bad characteristics. Bad characteristic is a characteristic which exceeds some threshold value of active bytes. So when it is found that differential characteristic reaches some threshold value it is dropped. It considerably simplifies the computation.

General formula for counting is represented below:

$$\begin{aligned} O &= N_{PT} N_{MK} N_{DC} = \\ &= N_{Col}^c N_{Col}^c \prod_{i=0}^r \prod_{j=0}^c N_{ij} = (N_{Col}^c)^2 \prod_{i=0}^r \prod_{j=0}^c N_{ij} \end{aligned} \quad (5)$$

Using formula 5 the total complexity for 128-bits version of cipher for all 10 rounds can be computed. It is expected that Shift Rows transformation creates 9 branches on each round.

In general there are 15 rounds (5 rounds of key-expansion scheme and 10 rounds of main loop of encryption).

The calculation for the 128-bits version of cipher is represented below:

$$O_{128} = N_{PT} N_{MK} N_{DC} = 9^2 9^2 9^{15} = 3^{57} \approx 2^{90}.$$

The complexity is very big but this complexity can be considerably reduced with filtering differential characteristic which exceeds some threshold. The minimal value for 128-bits version of cipher is 27 – this is minimal amount of active bytes which is allowed. So there are more than 27 active bytes in differential characteristic it is dropped.

On quad core system with AMD Phenom 3.2 Hz processor this algorithm takes a time about 10 minutes.

CONCLUSIONS

Method for security estimation of perspective SPN-based block cipher against related-key attacks are presented in this paper. The new cipher is based on the AES construction with redesigned key schedule for providing protection against such type of attacks. The cipher was proposed to the public competition of block cipher selection to be a prototype during development of Ukrainian National Standard [4,17].

Proposed method is based on counting amount of active bytes in differential characteristics. But unlike algorithm from Biryukov and Nikolic [11] which controls each byte of state, in the presented algorithm entire column is controlled for amount of active bytes in it without exact position of these bytes. Such scheme decreases the complexity of computation and reduces influence of high branching mentioned in [11].

Developed method can show existence of such differential characteristic which can lead to the key recovery with complexity lower then complexity of brute force attack.

Also the calculation of the complexity for the developed method is presented. This method with direct application has large computational complexity which is about $O = 2^{90}$ for 128-bits version of cipher. For modern computers such complexity is too big so some optimizations were performed. These optimizations are based on the dynamic elimination of differential characteristics which reach some threshold value of active bytes. Such optimization allows considerably reducing complexity. Optimized algorithm which is implemented in C++ language takes about 10 minutes for 128-bits version of cipher.

So proposed method of estimation gives the analytic proof of security to related key attacks. It was shown that 128-bits version of cipher does not have such differential characteristic which can lead to the key recovery with complexity which is low then complexity of brute force attack.

This method can be extended to different variants of block size and key lengths of proposed ciphers as well as to other block ciphers with similar structure.

References

- [1] Schneier Bruce «Applied Cryptography: Protocols, Algorithms, and Source», Code in C, Second Edition, John Wiley & Sons, 1994
- [2] Stallings William «Cryptography and Network Security: Principles and Practice», Prentice Hall, 2006
- [3] Federal Information Processing Standards Publication 197: Specification for the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001
- [4] R.V. Oliynykov, I.D. Gorbenko, V.I. Dolgov, V.I. Ruzhentsev. Perspective symmetric block cipher “Kalina” – basic terms and specification. Applied radioelectronics. Special issue which is devoted to the problems of information security. Kharkiv. Volume 6, № 2, 2007 // in Ukrainian
- [5] Alex Biryukov and Dmitry Khovratovich «Related-key Cryptanalysis of the Full AES-192 and AES-256», University of Luxembourg 29 May 2009, <http://impic.org/papers/Aes-192-256.pdf> / (visited 25.05.2014)

- [6] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, Adi Shamir «Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds», <http://eprint.iacr.org/2009/374.pdf> / (visited 25.05.2014)
- [7] Alex Biryukov, Dmitry Khovratovich, Ivica Nikoli «Distinguisher and Related-Key Attack on the Full AES-256», University of Luxembourg, 10 August 2009, <http://www.iacr.org/archive/crypt-2009/56770229/56770229.pdf> / (visited 25.05.2014)
- [8] I.D. Gorbenko «Information security in information and telecommunication systems» / Textbook. Part 1. Cryptographic protection of information – Kharkiv KNURE, 2004. – 368 p. // In Ukrainian
- [9] GOST 28147-89: Information processing systems. Cryptographic protection. Cryptographic transformation algorithm. // in Russian / <http://protect.gost.ru/document.aspx?control=7&id=139177> / (visited 25.05.2014)
- [10] R.V. Oliynykov, V.I. Ruzhentsev. A new approach of key schedule construction for symmetric block ciphers. Proceedings of the SFU. Engineering. «Information Security.» – Russia, Taganrog: Publisher TTISFU (Taganrog Technological Institute of Southern Federal University), 2010. № 11 (112), p.156–161.
- [11] Alex Biryukov, Ivica Nikoli «Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others»
- [12] M. Matsui. On correlation between the order of S-boxes and the strength of DES. In A. D. Santis, editor, EUROCRYPT, volume 950 of Lecture Notes in Computer Science, pages 366{375. Springer, 1994.
- [13] P.-A. Fouque, G. Leurent, and P. Nguyen. Automatic search of differential path in MD4. Cryptology ePrint Archive, Report 2007/206.
- [14] M. Stevens. Fast collision attack on MD5. Cryptology ePrint Archive, Report 2006/104.
- [15] C. D. Canniere and C. Rechberger. Finding SHA-1 characteristics: General results and applications. In X. Lai and K. Chen, editors, ASIACRYPT, volume 4284 of Lecture Notes in Computer Science, pages 1-20. Springer, 2006.
- [16] Howard M. Heys. A tutorial on linear and differential cryptanalysis. Cryptologia, Volume 26, Issue 3, July 2002, Pages 189–221.
- [17] Oliynykov, R., Gorbenko, I., Dolgov, V., & Ruzhentsev, V. (2010). Results of Ukrainian national public cryptographic competition. Tatra Mountains Mathematical Publications, 47(1), 99–113.

Поступила в редколлегию 10.06.2014



Олейников Роман Васильевич, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: анализ и синтез симметричных криптографических преобразований, безопасность программного обеспечения.



Кайдалов Дмитрий Сергеевич, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: анализ стойкости блочных симметричных шифров.

УДК 621.391:519.2:519.7

Криптоанализ перспективного симметричного блочного шифра с использованием связанных ключей / Р.В. Олейников, Д.С. Кайдалов // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 192–200.

Симметричные блочные шифры являются одними из наиболее распространенных криптографических примитивов. Кроме обеспечения конфиденциальности через шифрование, блочные шифры применяются как базовые компоненты при построении хэш-функций, кодов аутентификации сообщений, генераторов псевдослучайных чисел в составе различных криптографических протоколов и др. Одним из распространенных шифров в настоящее время является AES (Advanced Encryption Standard), используемый как стандарт симметричного шифрования во многих странах во всем мире. Несколько лет назад была предложена теоретическая атака против схемы разворачивания ключей AES, и сложность этой атаки оказалась значительно меньше по сравнению с полным перебором ключей. В статье рассмотрен метод оценки стойкости алгоритма шифрования к атаке на связанных ключах, и его применение для перспективного блочного шифра-кандидата на стандарт блочного шифрования в Украине.

Ключевые слова: блочный шифр, криптоанализ, атака на связанных ключах.

Табл.: 5. Ил.: 14. Библиогр.: 17 назв.

УДК 621.391:519.2:519.7

Криптоаналіз перспективного симетричного блокового шифру із застосуванням зв'язаних ключів / Р.В. Олійников, Д.С. Кайдалов // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 192–200.

Симетричні блокові шифри є одними з найпоширеніших криптографічних примітивів. Крім забезпечення конфіденційності через шифрування, блокові шифри застосовуються як базові компоненти в ході побудови геш-функцій, кодів автентифікації повідомлення, генераторів псевдовипадкових послідовностей, у складі різних криптографічних протоколів та ін. Одним із поширених шифрів зараз є AES (Advanced Encryption Standard), що використовується як стандарт у багатьох країнах світу. Декілька років тому була запропонована теоретична атака проти схеми розгортання ключів AES, і складність цієї атаки виявилася значно меншою порівняно із повним перебором ключів. У статті розглянуто метод оцінки складності алгоритму шифрування до атаки на зв'язаних ключах, і його застосування для перспективного блокового шифру-кандидата на стандарт блокового шифрування в Україні.

Ключові слова: блоковий шифр, криптоаналіз, атака на зв'язаних ключах.

Табл.: 5. Ил.: 14. Бібліогр.: 17 найм.

МОДЕЛИРОВАНИЕ ПЕРСПЕКТИВНОГО БЛОЧНОГО ШИФРА «КАЛИНА»

А.А. КУЗНЕЦОВ, Д.В. ИВАНЕНКО, Е.П. КОЛОВАНОВА

Рассматривается структура и основные базовые преобразования перспективного блочного шифра «Калина». Разрабатывается уменьшенная модель шифра посредством масштабирования основных криптопреобразований с сохранением их алгебраической структуры. Разработанная модель предназначена для проведения исследований основных характеристик шифра и прогнозирования уровня криптографической стойкости полной версии преобразований «Калина».

Ключевые слова: ключ, криптоалгоритм, уменьшенная версия шифра, схема разворачивания ключа.

ВВЕДЕНИЕ

В Украине последнее десятилетие в области криптографии стало особенным. Необходимость принятия нового стандарта блочного шифрования повлекло за собой проведение внутреннего конкурса по выдвижению кандидатов на национальный стандарт блочного симметричного шифрования (БСШ), где было представлено пять предложений [1–6]. Задача состояла не только в поиске убедительных теоретических обоснований принимаемых решений, но и в получении реальных практических результатов, что позволит накопить объективные данные для сравнительного анализа претендентов, сформулировать требования к проекту национального стандарта блочного симметричного шифрования на современном этапе развития криптографии [7].

Для преодоления трудностей анализа полномасштабных моделей (алгоритмов) шифрования в работах [8–10] было предложено пойти путем разработки и исследования уменьшенных моделей прототипов. Построение уменьшенных моделей, которые сохраняют все свои свойства, позволяет решить многие задачи анализа и сравнения по показателям стойкости соответствующих больших версий [11–13].

Задачей этой статьи является анализ одного из претендентов на национальный стандарт БСШ, а именно алгоритм «Калина» [14, 15], как дальнейшее развитие конкурсного предложения «Калина» [2], построение уменьшенной модели шифра посредством масштабирования основных криптопреобразований с сохранением их алгебраической структуры. Разрабатываемая модель предназначена для проведения исследований основных характеристик шифра и прогнозирования уровня криптографической стойкости полной версии преобразований «Калина» [14, 15].

1. БСШ «КАЛИНА»

Шифр «Калина» является дальнейшим развитием БСШ «Калина», который, в свою очередь, разрабатывался на основе известной структуры «квадрат» БСШ Rijndael [16].

В шифре «Калина» сохранены все базовые операции шифра «Rijndael», основные отличия состоят в использовании разных S-блоков (используются 4 различных S-блока), сгенериро-

ванных случайным образом, вместо одинаковых S-блоков, и в применении попеременного сложения с цикловыми подключами по модулю 2 и по модулю 2^{64} . Кроме того, линейное преобразование выполняется с помощью матрицы МДР кода размера 8×8 над полем $GF(2^8)$, что также потенциально улучшает криптографические свойства шифра. Параметры шифра «Калина» представлены в табл. 1.

Таблица 1

Характеристики шифра «Калина»

Key length Block size	128 ($N_k = 2$)	256 ($N_k = 4$)	512 ($N_k = 8$)
128 ($N_b = 2$)	10	14	—
256 ($N_b = 4$)	—	14	18
512 ($N_b = 8$)	—	—	18

1.1 Алгоритм шифрования. Схема шифрования (см. рис. 1) БСШ «Калина» обладает следующими особенностями:

- процедура забеливания выполняется с помощью сложения с нулевым подключом по модулю 2^{64} ;
- в циклах от первого до $N_r - 1$ цикловые подключи вводятся с помощью операции побитового сложения по модулю 2;
- на последнем цикле шифрования выполняется очередное цикловое преобразование SubBytes, ShiftRows, MixColumns и сложение с цикловым подключом по модулю 2^{64} ;
- в шифре «Калина» применяется четыре разных S-блока.

1.2 Схема разворачивания ключей. В шифре «Калина» предложена новая, более эффективная схема разворачивания ключей. При шифровании используется $N_r + 1$ цикловых ключей k_i ($i = 0, 1, \dots, N_r$), каждый длиной $64 \times N_b$ бит (размер циклового ключа совпадает с размером открытого текста/шифртекста и текущего состояния шифра). Алгоритм разворачивания ключа можно представить в виде последовательного выполнения трех этапов (процедур):

- 1) из ключа шифрования формируется промежуточный ключ K_i длиной, равной размеру блока ($64 \times N_b$ бит), с применением трех циклов шифрования;

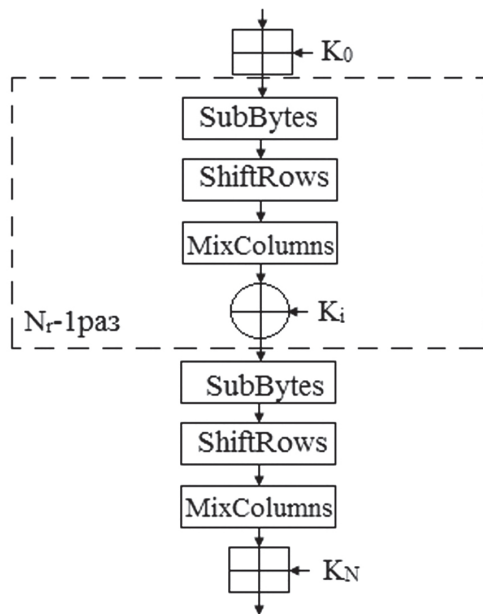


Рис. 1. Схема шифрования шифра «Калина»

2) на основе ключа шифрования K и промежуточного ключа K_i формируются цикловые ключи k_{2i} (с четными индексами) с длинами, равными размеру блока ($64 \times N_b$ бит), с применением двух циклов шифрования для каждого циклового ключа;

3) из цикловых ключей k_{2i} с четными индексами формируются цикловые ключи k_{2i+1} (с нечетными индексами) путем циклического сдвига предыдущего ключа с четным индексом влево на $(2N_b + 3)$ байта.

Схема разворачивания ключей представлена на рис. 2.

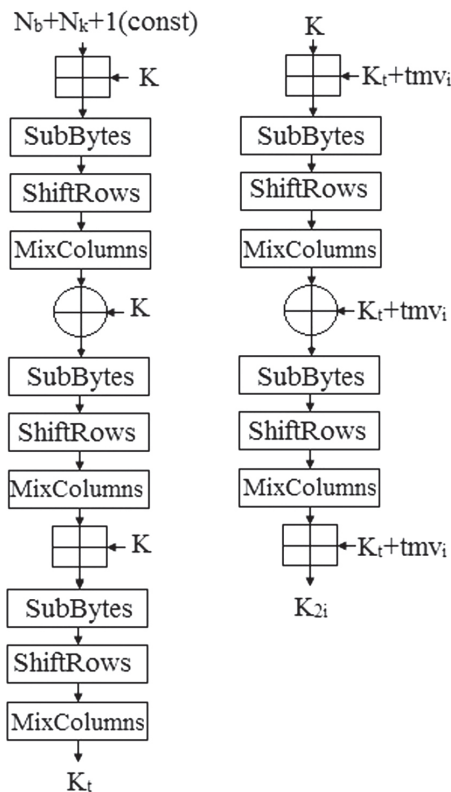


Рис. 2. Схема разворачивания ключей

1.2.1 Формирование промежуточного ключа K_i .

Промежуточный ключ K_i имеет длину $64 \times N_b$ бит (совпадает по размеру с длиной блока открытого текста) и формируется на основе ключа шифрования K длиной $64 \times N_k$ бит с использованием преобразований, использованных при построении цикловых функций.

Для формирования K_i выполняются три цикла шифрования. На вход трёхциклового преобразования (с начальным забеливанием) подается двоичное число (в нулевое состояние заносится арифметическая сумма $N_b + N_k + 1$, остальные байты заполняются нулями), определяемое текущим размером блока и длиной ключа, а в качестве цикловых ключей используется ключ шифрования (или его младшая и старшая половины, если ключ длиннее блока). Значение, полученное на выходе преобразования, является промежуточным ключом K_i .

1.2.2 Формирование цикловых ключей с четными индексами.

При генерации цикловых ключей с четными индексами ключ шифрования K или его циклический сдвиг подаются на двухцикловое преобразование (с начальным забеливанием и операцией *Add64RoundKey* во втором цикле) как открытый текст (один или два блока, в зависимости от длины формируемого ключа). В качестве циклового ключа используется результат обработки промежуточного ключа K_i функцией *Add64RoundKey* (сложение K_i по модулю 2^{64} со вторым аргументом), где вторым аргументом является значение (двоичное число), зависящее от индекса формируемого циклового ключа (переменная tmv_i).

Размер переменной tmv_i равен длине блока. Константа формируется повторением байтов 0x01, 0x00 (в шестнадцатеричном представлении) до заполнения состояния.

При переходе к формированию очередного циклового ключа с четными индексами производится модификация переменной tmv_i с помощью операции *ShiftLeft*, которая обрабатывает состояние шифра (значение переменной tmv_i) как последовательность 64-битных слов. Каждое слово состояния ($w_0, w_1, \dots, w_{N_b-1}$) с каждым циклом преобразования логически сдвигается влево на 1 бит, т.е. $w_i = 2 w_i (\text{mod } 2^{64})$.

Результирующие цикловые ключи с четными индексами формируются из состояний на выходе двухцикловых преобразований с помощью операции *Rotate*, которая обрабатывает состояние как последовательность 64-битных слов ($w_0, w_1, \dots, w_{N_b-1}$), выполняя циклический сдвиг и возвращая состояние ($w_1, \dots, w_{N_b-1}, w_0$).

1.2.3 Формирование цикловых ключей с нечетными индексами.

Каждый из цикловых ключей с четным индексом, полученный на предыдущем этапе процедуры генерации, представляется в виде байтовой строки. Эта строка циклически сдвигается влево на $2N_b + 3$ байта, и затем снова представляется в виде состояния, которое ис-

пользуется как цикловый ключ с нечетным индексом, т.е. $k_{2i+1} = k_{2i} < \ll (2N_k + 3)$.

Таким образом, байтовая строка $b_0, b_1, \dots, b_{8N_b-1}$ после преобразования приобретает вид $b_{2N_b+3}, b_{2N_b+4}, \dots, b_{8N_b-1}, b_0, b_1, \dots, b_{2N_b+2}$.

Зависимость константы, определяющей значение сдвига влево циклового ключа с четным индексом, от размера блока, приведена в табл. 2.

Таблица 2

Константа, определяющая значение сдвига влево циклового ключа с четным индексом, в зависимости от размера блока

Размер блока, бит (байт)	Сдвиг влево (байт)
128 (16)	7
256 (32)	11
512 (64)	19

2. РАЗРАБОТКА УМЕНЬШЕННОЙ МОДЕЛИ БСП «КАЛИНА»

Алгоритм шифрования мини-Калина повторяет принципиальные решения, использованные при построении полной версии шифра «Калина» и практически является результатом масштабирования оригинальной разработки к размеру входного блока и ключа равному 16 битам (см. табл. 3, а) и 3, б)).

Таблица 3.а)

Представление 16-битного слова,
 $P=36=\{0010,0100,0000,0000\}_2$

P ₀				P ₁				P ₂				P ₃			
bit	bit	bit	bit	bit	bit	bit	bit	bit	bit	bit	bit	bit	bit	bit	bit
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0

Таблица 3.б)

Представление 16-битного слова

P ₀	P ₂
P ₁	P ₃

Миниверсия «Калина» практически полностью повторяет решения по построению функций ShiftRows, MixColumn шифра miniAES [9, 10], слой нелинейного преобразования реализован с помощью двух S-блоков. Рассмотрим особенности построения отдельных слоев преобразования миниверсии БСП «Калина».

2.1 NibbleSub. NibbleSub – это простая операция подстановки Nibble в Nibble, где Nibble – 4-битное слово. Блок представляется в виде матрицы 2×2 Nibble. Главное отличие разрабатываемой миниверсии от miniAES [9, 10] состоит в использовании двух таблиц (см. табл. 4) подстановок: первая таблица для $\{P_0, P_1\}$, вторая – для $\{P_2, P_3\}$.

На вход блока NibbleSub подается множество P ($P=\{P_0, P_1, P_2, P_3\}$), на выходе блока получаем множество A ($A=\{a_0, a_1, a_2, a_3\}$) (см. рис. 3).

Пример 1: на вход подано множество $P=\{1101, 0111, 1010, 0110\}$, на выходе получаем множество $A=\{0010, 1110, 0111, 1100\}=\{2, 14, 7, 12\}$.

Таблица 4

Sbox для NibbleSub

		P ₀ , P ₁	P ₂ , P ₃
0	0000	10	10
1	0001	13	15
2	0010	1	14
3	0011	3	9
4	0100	12	2
5	0101	4	1
6	0110	6	11
7	0111	14	5
8	1000	9	0
9	1001	5	12
10	1010	11	7
11	1011	0	3
12	1100	7	6
13	1101	2	4
14	1110	8	13
15	1111	15	8

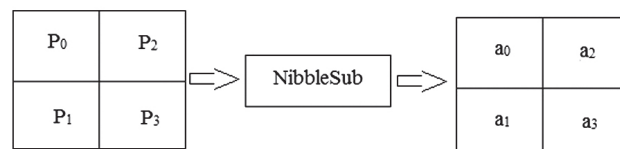


Рис. 3. Пример подстановки

2.2 ShiftRow. Блок ShiftRow меняет местами P_3 и P_1 входного блока, оставляя их без изменения. P_2 и P_0 остаются без изменения. Иллюстрацию примера можно посмотреть на рис. 4.

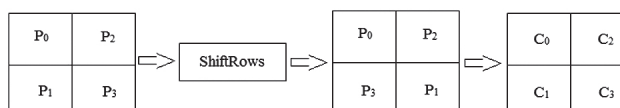


Рис. 4. Операция ShiftRow

Пример 2: на вход блока подано $P=\{P_0, P_1, P_2, P_3\}$ на выходе блока получим $C=\{C_0, C_1, C_2, C_3\}=\{P_0, P_3, P_2, P_1\}$.

2.3 MixColumn. Блок MixColumn – это перемножение входной матрицы на матрицу-константу, получая матрицу на выходе (рис. 5), где $P=\{P_0, P_1, P_2, P_3\}$ подается на вход, $C=\{C_0, C_1, C_2, C_3\}$ получается на выходе, соответственно. Умножение элементов происходит в поле $GF(2^4)$, которое построено на полиноме x^4+x+1 .

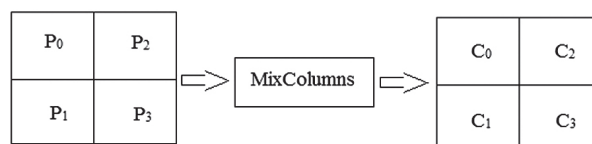


Рис. 5. Операция MixColumn

Матрица-константа, определяющая преобразование MixColumn, имеет вид: $\begin{bmatrix} 10 & 7 \\ 7 & 15 \end{bmatrix}$.

Пример 3: Пусть $P=\{P_0, P_1, P_2, P_3\}$ входной блок и $C=\{C_0, C_1, C_2, C_3\}$ выходной блок. Если

входной блок P , матрица 2×2 , тогда первый столбец умножается на матрицу-константу. На выходе получим столбец:

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} 10 & 7 \\ 7 & 15 \end{bmatrix} \begin{bmatrix} P_0 \\ P_1 \end{bmatrix},$$

где

$$C_0 = (1010 \otimes P_0) \oplus (0111 \otimes P_1)$$

$$\text{и } C_1 = (0111 \otimes P_0) \oplus (1111 \otimes P_1).$$

Следующим шагом является нахождение второго столбца C , для этого второй столбец умножается на константу-матрицу:

$$\begin{bmatrix} c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 10 & 7 \\ 7 & 15 \end{bmatrix} \begin{bmatrix} P_2 \\ P_3 \end{bmatrix},$$

где

$$C_2 = (1010 \otimes P_2) \oplus (0111 \otimes P_3)$$

$$\text{и } C_3 = (0111 \otimes P_2) \oplus (1111 \otimes P_3).$$

2.4 KeyAddition. В блоке KeyAddition входное сообщение складывается с ключом по модулю 2^8 . 16-битное входное сообщение делится на два байта и побайтно складывается с 16-битным ключом, результат берется по модулю 2^8 , затем результат конкатенируется.

Пример 4: Пусть $P = \{P_0, P_1, P_2, P_3\} = \{1111, 0011, 0011, 1011\}$ входное сообщение и $K = \{K_0, K_1, K_2, K_3\} = \{1010, 1101, 1111, 1001\}$ ключ. Представим входное сообщение и ключ в виде двух байтов:

$$P = (11110011, 00111011) \text{ и } K = \{10101101, 11111001\}$$

Тогда выходное сообщение C :

$$C = (\{11110011 + 10101101\} \parallel \{00111011 + 11111001\}) = (1010, 0000, 0011, 0100).$$

2.5 XorRoundKey. В блоке XorRoundKey 16-битное входное сообщение складывается с 16-битным ключом, соответствующего раунда, по модулю 2. Полученное сообщение подается на выход.

Пример 5: Пусть $P = \{P_0, P_1, P_2, P_3\} = \{1111, 0011, 0011, 1011\}$ входное сообщение и $K = \{K_0, K_1, K_2, K_3\} = \{1010, 1101, 1111, 1001\}$ ключ. Тогда выходное сообщение C будет иметь вид:

$$C = P \oplus K = (0101, 1110, 1100, 0010).$$

2.6 Схема разворачивания ключей. При шифровании (см. рис. 1) используется $N_r + 1$ цикловых ключей k_i ($i = 0, 1, \dots, N_r$), каждый длиной $8 \times N_b$ бит (размер циклового ключа совпадает с размером открытого текста/шифртекста и текущего состояния шифра).

Алгоритм разворачивания ключа можно представить в виде последовательного выполнения трёх этапов (трёх процедур):

1) из ключа шифрования формируется промежуточный ключ K_i длиной, равной размеру блока ($8 \times N_b$ бит), с применением трех циклов шифрования;

2) на основе ключа шифрования K и промежуточного ключа K_i формируются цикловые ключи k_{2i} (с четными индексами) с длинами, равными

размеру блока ($8 \times N_b$ бит), с применением двух циклов шифрования для каждого циклового ключа;

3) из цикловых ключей k_{2i} с четными индексами формируются цикловые ключи k_{2i+1} (с нечетными индексами) путем циклического сдвига предыдущего ключа с четным индексом влево на $(2N_b + 3)$ бита.

2.6.1. Формирование промежуточного ключа K_i . Промежуточный ключ K_i имеет длину $8 \times N_b$ бит (совпадает по размеру с длиной блока открытого текста) и формируется на основе ключа шифрования K длиной $8 \times N_k$ бит с использованием преобразований, использованных при построении цикловых функций.

Для формирования K_i выполняются три цикла шифрования. На вход трехциклового преобразования (с начальным забеливанием) подается двоичное число, определяемое текущим размером блока и длиной ключа (арифметическая сумма $(N_b + N_k + 1)$, в остальные биты заполняются 0), а в качестве цикловых ключей используется ключ шифрования (или его младшая и старшая половины, если ключ длиннее блока). Значение, полученное на выходе преобразования, является промежуточным ключом K_i .

2.6.2. Формирование цикловых ключей с четными индексами. При генерации цикловых ключей с четными индексами ключ шифрования K или его циклический сдвиг подаются на двухциклового преобразования (с начальным забеливанием и операцией *AddRoundKey* во втором цикле) как открытый текст (один или два блока, в зависимости от длины формируемого ключа). В качестве циклового ключа используется результат обработки промежуточного ключа K_i функцией *AddRoundKey* (сложение K_i по модулю 2^8 со вторым аргументом), где вторым аргументом является значение (двоичное число), зависящее от индекса формируемого циклового ключа (переменная tmv_i).

Размер переменной tmv_i равен длине блока. Константа формируется повторением битов $\{01\}$, $\{00\}$ до заполнения состояния.

При переходе к формированию очередного циклового ключа с четными индексами производится модификация переменной tmv_i с помощью операции *ShiftLeft*, слово состояния ($w_0, w_1, \dots, w_{N_b-1}$) с каждым циклом преобразования логически сдвигается влево на 1 бит, т.е. $w_i = 2 w_i \pmod{2^{16}}$.

2.6.3 Формирование цикловых ключей с нечетными индексами. Каждый из цикловых ключей с четным индексом, полученный на предыдущем этапе процедуры генерации, представляется в виде 16-битной строки. Эта строка циклически сдвигается влево на $(2N_b + 3)$ бита, и затем снова представляется в виде состояния, которое используется как цикловой ключ с нечетным индексом, т.е. $k_{2i+1} = k_{2i} \ll (2N_b + 3)$.

Для данного случая $N_b = 2$, следовательно, константа, определяющая значение сдвига влево циклового ключа с четным индексом, равна 7.

ВЫВОДЫ

Проведенный анализ структуры и основных базовых преобразований БСШ «Калина» показал, что данный криптоалгоритм имеет ярко выраженную алгебраическую структуру, которая унаследована от алгоритмов-прототипов «Калина» и «Rijndael» [2, 16]. В частности, алгоритм «Калина» имеет структуру «квадрат», при этом значение состояния шифра представляется матрицей из восьми строк и $N_b \in \{2, 4, 8\}$ столбцов (в зависимости от размера блока (128, 256, 512 бит) шифрования). Основным отличием от БСШ «Rijndael» является увеличенный размер состояния (восемь строк вместо четырех) с использованием увеличенной матрицы рассеивания (на основе матрицы МДР кода размера 8×8 вместо 4×4 для БСШ «Rijndael»), а также использованием нескольких нелинейных узлов замен, сформированных случайным образом (вместо алгебраической структуры S-блоков шифра «Rijndael»). По сравнению с БСШ «Калина» новый алгоритм шифрования «Калина» отличается усовершенствованной схемой разворачивания ключей, а также новыми S-блоками с улучшенными криптографическими свойствами.

Разработанная уменьшенная модель шифра «Калина» сохраняет алгебраическую структуру алгоритма-прототипа. Посредством масштабирования основных криптографических преобразований удастся моделировать базовые преобразования и исследовать их характеристики. В частности, переход к 16-битной версии шифра позволяет исследовать дифференциальные и линейные свойства шифрующего преобразования, производить соответствующую оценку стойкости к криптоаналитическим атакам, посредством переноса и интерпретации полученных результатов на полную версию алгоритма «Калина» прогнозировать поведение БСШ в случае применения различных методов криптоанализа, т.е. давать оценку уровня криптографической стойкости полной версии БСШ «Калина». В приложении А представлены примеры расчетов с различными входными данными, согласно разработанной миниверсии «Калина».

Перспективным направлением дальнейших исследований является разработка программной реализации мини-версии БСШ «Калина», проверка адекватности уменьшенной модели, исследование дифференциальных и линейных свойств криптоалгоритма с прогнозированием уровня стойкости к криптоаналитическим атакам.

Литература

- [1] Положення про проведення відкритого конкурсу криптографічних алгоритмів. <http://dstszi.gov.ua/dstszi/control/uk/publish/>, 2006.
- [2] Горбенко І.Д. Перспективний блоковий симетричний шифр «Калина» / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та ін. // Прикладна радіоелектроніка. — 2007. — Т. 6. — № 2. — С. 195–208.
- [3] Головашич С.А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. — Харьков: ХТУРЭ. — 2007. — Том. 6, №2. — С. 230–240.
- [4] Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор» — основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов та ін. // Прикладна радіоелектроніка — Харьков: ХТУРЭ. — 2007. — Том. 6, №2. — С. 147–157.
- [5] Кузнецов А.А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption). / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко // Прикладная радиоэлектроника. — Харьков: ХТУРЭ. — 2007. — Том 6, №2 — С. 241–249.
- [6] Белецкий А.Я. Семейство симметричных блочных RSB криптографических алгоритмов с динамически управляемыми параметрами шифрования / А.Я. Белецкий, А.А. Белецкий, А.А. Кузнецов // Електроніка та системи управління. — 2007. — № 1 (11). — С. 5–16.
- [7] Горбенко І.Д. Стандартизація алгоритмів шифрування. Требования к проекту национального стандарта блочного симметричного шифрования на современном этапе развития криптографии. / И.В. Горбенко, И.В. Лисицкая // Радиотехника. Всеукр. міжвед. научн.-техн. сб. — 2011. — Вып. 166. — С. 5–10.
- [8] A Description of Baby Rijndael // ISU CprE/Math 533; NTU ST765-U. — 2003.
- [9] Raphael Chung-Wei Phan. Mini Advanced Encryption Standard (Mini-AES): A testbed for Cryptanalysis Students / Raphael Chung-Wei Phan // Cryptologia. — October 2002. — XXVI(4). — P. 283–306.
- [10] Raphael Chung-Wei Phan. Impossible Differential Cryptanalysis of Mini-AES / Raphael Chung-Wei Phan // Cryptologia. — October 2003. — XXVII(4). — P. 361–374.
- [11] Долгов В.И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс. / В.И. Долгов, А.А. Кузнецов, С.А. Исаев. // Электронное моделирование. — 2011. — Т. 33, № 6. — С. 81–99.
- [12] Долгов В.И. Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES / В.И. Долгов, А.А. Кузнецов, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника. — Харьков: ХНУРЭ. — 2009. — Т. 8, № 3. — С. 252–257.
- [13] Кузнецов А.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. — 2011. — Т. 10, № 2 — С. 135–140.
- [14] Проект стандарту ДСТУ "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення", друга (остаточна) редакція, Харків: АТ «ІТ», 238 с.
- [15] Розробка нового блокового симетричного шифру: звіт за перший етап НДР «Алгоритм» (промисловий) / АТ «ІТ»; кер. Горбенко І.Д.; викон.: Олейніков Р.В. [та ін.]. — Харків, 2014. — Т. 4. — 304 с.
- [16] J. Daemen and V. Rijmen. The Design of Rijndael: AES — the Advanced Encryption Standard, Springer-Verlag, Berlin, 2002.

Поступила в редколлегию 18.06.2014

ПРИЛОЖЕНИЕ А

Таблица А.1

Расчеты для схемы разворачивания ключей для четырехраундовой мини-версии «Калина» для разных ключей, при const=5 и $Tmv_0=8738$

	Key=5	Key=10	key=6405	key=58723
1	2	3	4	5
Add(const,key)	0101000000000000	1111000000000000	0101000010011000	0001011010100111
NibbleBox	0100101010101010	1111101010101010	0100101011000000	1101011001110101
ShiftRow	0100101010101010	1111101010101010	0100000011001010	1101010101110110
MixColumn	1101001110111111	1111011110111111	1110111100101110	0011001100100010
Xor(state,key)	0111001110111111	1010011110111111	0100111110110110	1111010110000101
NibbleBox	1110001100111000	1011111000111000	1100111100111011	1111010000000001
ShiftRow	1110100000110011	1011100000111110	1100101100111111	1111000100000100
MixColumn	1011110101001011	1111010100011100	0101000101100011	1011010011111001
Add(state,key)	0100001101001011	1001110100011100	1111000111111011	0000100100100001
NibbleBox	1100001100100011	0101001011110110	1111110110000011	1010010111101111
ShiftRow	1100001100100011	0101011011110010	1111001110001101	1010111111100101
MixColumn	1000000011101100	0101110000100110	0101100110101010	0011100111101010
KS	1000000011101100	0101110000100110	0101100110101010	0011100111101010
1ая пара ключей	1round	1round	1round	1round
Add(KS, Tmv_0)	1100010010011010	0011101001100001	0011110111101110	0111110110011110
Add(KS Tmv_0 ,key)	0001010010011010	0110011001100001	1000001100001001	1000010001111010
NibbleBox	1101110011000111	0110011010111111	1001001110101100	1001110001010111
ShiftRow	1101011111001100	0110111110110110	1001110010100011	1001011101011100
MixColumn	1101111000111010	0010101100110000	0111001000010001	0011000101100000
Xor(state,KS Tmv_0)	0001101010100000	0001000101010001	0100111111111111	0100110011111110
NibbleBox	1101101101111010	1101110100011111	1100111110001000	1100011110001101
ShiftRow	1101101001111011	1101111000111011	1100100010001111	1100110110000111
MixColumn	1000100101110101	0000111111110000	1100001101000111	0100010110010110
Key0=				
Add(state,KS Tmv_0)	0010110111110000	0011001010101001	1111111010011010	0000011001000111
Key1=Key0<<<7	1111000000010110	0101010010011001	0100110101111111	0010001110000011
$Tmv_1=Tmv_0<<1$	1000100010001000	1000100010001000	1000100010001000	1000100010001000
2ая пара ключей	1round	1round	1round	1round
Add(KS, Tmv_1)	0100100000010010	1101001010101110	1101010101100110	1011010100010110
Add(KS Tmv_1 ,key)	1110100000010010	1010101010101110	0000110111111110	0000100010110010
NibbleBox	1000100111111110	1011101101111101	1010001010001101	1010100100111110
ShiftRow	1000111011111001	1011110101111011	1010110110000010	1010111000111001
MixColumn	0011100001100101	0111001101110101	1101010000010000	0100011001110111
Xor(state,KS Tmv_1)	0111000001110111	1010000111011011	0000000101110110	1111001101100001
NibbleBox	1110101001010101	1011110101000011	1010110101011011	1111001110111111
ShiftRow	1110010101011010	1011001101001101	1010101101011101	1111111110110011
MixColumn	1110101001110100	1011011010111000	1100000000011111	0111000110110110
Key2=				
Add(state,KS Tmv_1)	1001011001101110	0001110101001001	0111010101111010	1101110010101011
Key3=Key2<<<7	0011011101001011	1010010010001110	1011110100111010	0101010111101110
$Tmv_2=Tmv_1<<1$	0001000100010000	0001000100010000	0001000100010000	0001000100010000
3ая пара ключей	1round	1round	1round	1round
Add(KS, Tmv_2)	1001000111111100	0100001100110110	0100010010111010	0010010011111010
Add(KS Tmv_2 ,key)	0111000111111100	0011001100110110	1110010001101110	1110000100100010
NibbleBox	1110110110000110	0011001110011011	1000110010111101	1000110111101110
ShiftRow	1110011010001101	0011101110010011	1000110110111100	1000111011101101
MixColumn	0111100010101010	1001101011001000	1010101000001100	0011100000111011
Xor(state,KS Tmv_2)	1110100101010110	1101100111111110	1110111010110110	0001110011000001
NibbleBox	1000010100011011	0010010110001101	1000100000111011	1101011101101111
ShiftRow	1000101100010101	0010110110000101	1000101100111000	1101111101100111
MixColumn	1011111000100001	0010100101111011	1011111000001000	0000111111111010
Key4=				
Add(state,KS Tmv_2)	01110000011000011	0110101001010010	1111100110110110	0010100001111101
Key5=Key4<<<7				
	0110000110110000	0010100100110101	1101101101111100	0011111010010100

Таблица А.1

Шифрование четырехраундовой мини-версии «Калина» разных входных сообщений,
при const=5, Tmv₀=8738 и key=5

	plaintext=10241	plaintext=15966	plaintext=56343	plaintext=2204
	round 0	round 0	round 0	round 0
Add(plaintext,key0)	1010110111110100	0100100010100010	11010011111000111	0000101011110000
	round 1	round 1	round 1	round 1
NibbleBox	1011001010000010	1100100101111110	0010001101100101	1010101110001010
ShiftRow	1011001010000010	11001110011111001	0010010101100011	1010101010001011
MixColumn	1100100100010000	1101011110011000	1111100000000011	1011111110111110
Xor(state,roundKey1)	0011100100000110	0010011110001110	0000100000010101	0100111110101000
	round 2	round 2	round 2	round 2
NibbleBox	0011010110101011	0001111000001101	1010100111110001	1100111101110000
ShiftRow	0011101110100101	0001110100001110	1010000111111001	1100000001111111
MixColumn	1001101000000101	1111000011000101	111110001100101	0001001010001100
Xor(state,roundKey2)	0000110001101011	0110011010101011	0110101000001011	1000010011100010
	round 3	round 3	round 3	round 3
NibbleBox	1010011110110011	0110011001110011	0110101110100011	1001110011011110
ShiftRow	1010001110110111	0110001101110110	0110001110101011	1001111011011100
MixColumn	0001000101001111	0000001100100010	0000001111000000	1001111110011101
Xor(state,roundKey3)	0010011000000100	0011010001101001	0011010010001011	1010100011010110
	round 4	round 4	round 4	round 4
NibbleBox	0001011010100010	0011110010111100	0011110000000011	1011100101001011
ShiftRow	0001001010100110	0011110010111100	0011001100001100	1011101101001001
MixColumn	0100101010010111	1111000100001100	0100101100101000	0110011101000001
Add(state,roundKey4)	0001101000110101	1010100111001111	0001101111101011	0011011110100010



Кузнецов Александр Александрович, доктор технических наук, профессор кафедры БИСТ ХНУ им. В.Н. Каразина. Научные интересы: криптография, теория обработки и передачи данных, стеганографические методы защиты информации.



Иваненко Дмитрий Викторович, кандидат технических наук, старший преподаватель кафедры БИТ ХНУРЭ. Научные интересы: криптография, атаки по сторонним каналам, анализ стойкости блочных симметричных шифров.



Колованова Евгения Павловна, ведущий инженер кафедры БИТ ХНУРЭ. Научные интересы: криптография и аутентификация, анализ стойкости блочных симметричных шифров.

УДК 004.056.55

Моделирование перспективного блочного шифра «Калина»/ О.О. Кузнецов, Д.В. Иваненко, Е.П. Колованова // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 201–207.

Розглядається структура та загальні базові перетворення перспективного блокового шифру «Калина». Розробляється зменшена модель шифру шляхом масштабування загальних криптоперетворень зі збереженням їх алгебраїчної структури. Розроблена модель призначена для проведення дослідження загальних характеристик шифру та прогнозування рівня криптографічної стійкості повної версії перетворень «Калина».

Ключові слова: ключ, криптоалгоритм, зменшена версія шифру, схема розгортання.

Табл.: 5. Іл.: 5. Бібліогр.: 16 найм.

UDC 004.056.55

Perspective block cipher «Kalyna» modelling / A.A. Kuznetsov, D.V. Ivanenko, E.P. Kolovanova // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 201–207.

The structure and common basic transformations of the perspective block cipher «Kalyna» are considered in this paper. A cipher mini-model is developed by scaling common cipher cryptotransformations with preservation of their algebraic structure. The developed mini-model is designed for studying the general cipher characteristics and forecasting the level of cryptographic strength for the full version of «Kalyna» transformations.

Keywords: key, cryptoalgorithm, minicipher, key schedule.

Tab.: 5. Fig.: 5. Ref.: 16 items.

СНОВА ОБ ОПТИМАЛЬНЫХ S-БЛОКАХ

К.Е. ЛИСИЦКИЙ

Приводятся результаты оценки динамических показателей процесса прихода шифра Хейза и уменьшенной модели шифра Rijndael по дифференциальным показателям к стационарным состояниям, свойственным случайным подстановкам при использовании в шифрах полубайтовых подстановок, сконструированных различными способами. Показано, что предлагаемый в одной из последних публикаций метод формирования оптимальных Q-S-блоков с использованием квазигрупп на самом деле не приводит к подстановкам с улучшенными криптографическими показателями. Делается вывод, что поиск полубайтовых S-блоков с улучшенными свойствами потерял смысл. Лучшие подстановочные преобразования уже получены на основе полного перебора всего множества полубайтовых подстановок симметрической группы.

Ключевые слова: подстановка, оптимальный S-блок, динамические показатели шифра, максимумы полных дифференциалов.

ВВЕДЕНИЕ

В научных публикациях уже поднимался вопрос о не перспективности направления, интенсивно развиваемого в криптографии, связанного с разработкой математических методов конструирования S-блоков с улучшенными криптографическими показателями, которые, как правило, ищут среди подстановок с минимально возможными значениями дифференциальных и линейных вероятностей. Этот вывод основывается на многочисленных экспериментах с уменьшенными моделями большого числа современных шифров. Результаты экспериментов свидетельствуют о том, что показатели стойкости шифров к атакам дифференциального и линейного криптоанализа от свойств используемых S-блоков практически не зависят [1] (за исключением шифра DES и близких к нему, допускающих использование при построении дифференциальных характеристик цикловых переходов обнуляющего типа).

Если говорить об эффективности подстановочного преобразования, то она определяется совместно с шифрующим преобразованием с помощью динамических показателей, в качестве которых выступают оценки числа циклов шифра, необходимых ему для перехода к стационарному состоянию, свойственному случайной подстановке соответствующей степени [2]. Речь идёт о числе циклов зашифрования, после которого законы распределения переходов таблиц XOR разностей и смещений таблиц линейных аппроксимаций шифра начинают повторять соответствующие законы распределения вероятностей случайных подстановок. И здесь оказывается, что во многих случаях S-блоки и не с минимальными значениями вероятностей дифференциальных и линейных характеристик обеспечивают наилучшие динамические свойства. В частности, в [1] показано, что в качестве S-блоков практически всех современных шифров могут выступать подстановки случайного типа. Именно процесс прихода к стационарному состоянию, характери-

зуемый числом циклов шифрования, является объективным свидетельством качества шифрующего преобразования в целом, а, следовательно, и используемых в шифре подстановочных преобразований.

Недавно появилась ещё одна публикация [3], в которой авторы претендуют на создание новой методики конструирования полубайтовых S-блоков с улучшенными криптографическими свойствами. В противовес работе [4], в которой «идеальные» S-блоки получены путём полного перебора всего множества полубайтовых подстановок, они претендуют на создание математического аппарата получения S-блоков с предельными, как они считают, криптографическими показателями.

В этой работе воспользуемся ещё одной возможностью продемонстрировать, во-первых, — далеко не лучшие свойства предлагаемых в [3] конструкций S-блоков в отношении реализации оптимальной динамики шифрующих преобразований, в которых они участвуют, а во-вторых, — ещё раз заострить внимание на том, что для полубайтовых подстановок вопрос с построением оптимальных конструкций уже полностью решён.

В первой части статьи приводится краткая характеристика предлагаемого в работе [3] метода и выделяются результативные её моменты. Во второй части излагаются результаты статистических экспериментов по оценке динамических свойств шифра Хейза со слабым линейным преобразованием и шифра Rijndael с сильным линейным преобразованием при использовании в этих шифрах подстановок различных конструкций, в том числе и подстановок, полученных с помощью предлагаемого в работе [3] метода.

1. КРАТКАЯ ХАРАКТЕРИСТИКА РЕЗУЛЬТАТОВ РАБОТЫ [3]

В своей работе авторы сосредотачиваются на так называемой легкой (lightweight) симметричной криптографии. Несмотря на то, что блочный шифр AES (Advanced Encryption

Standard) является одним из наиболее используемых криптографических примитивов, он в основном предназначен для эффективной программной реализации. Для многих ограниченных сред (применений), использование AES в качестве блочного шифра является либо слишком дорогим, либо нет необходимости для такого высокого уровня безопасности, который предлагает этот шифр. Поэтому, не удивительно, что в последние несколько лет наблюдается динамичное развитие в области легковесной криптографии, особенно в области легких блочных шифров, таких как PRESENT [4–5].

Основой безопасности в симметричной криптографии, почти во всех современных блочных шифрах, являются подстановки, известные также как S-блоки. S-блоки работают с небольшим набором данных, поэтому они должны отличаться высокими нелинейными свойствами, если хотят, чтобы они запутывали входные данные в шифре. PRESENT является ультра-легким блочным шифром, предложенным Богдановым и др. [2]. Отмечается, что он был разработан для чрезвычайных условий в виде весьма ограниченных ресурсов, таких как метки RFID (англ. Radio Frequency IDentification). Приводится краткое описание шифра. PRESENT является SPN блочным шифром, который состоит из 31 цикла и работает на 64-битных блоках данных. Он поддерживает две длины ключа 80 или 128 бит, где 80-битный ключ рекомендуется к использованию. Каждый из 31 циклов выполняется за три этапа (слоя). На первом этапе осуществляется сложение блока данных с цикловым подключом – AddRoundKey, второй этап – слой подстановок – SBoxLayer, и третий этап является битовой перестановкой pLayer. Наиболее интересным является второй этап, где главная роль принадлежит S-блокам. В нелинейном слое (SBoxLayer) используются одинаковые 4×4-битные S-блоки. Выбор 4×4-битных S-блоков является прямым следствием преследования авторами цели повышения эффективности применяемого оборудования, где реализация таких S-блоков, как правило, является гораздо более компактной и требует меньше ресурсов, чем 8×8-битные S-блоки. 4-битные S-блоки требуют менее четверти аппаратных затрат по сравнению с 8-битными S-блоками.

С точки зрения криптографии, 4-битные S-блоки должны выбираться очень тщательно, потому что они слабее, чем 8-битные S-блоки.

Далее отмечается, что S-блоки шифра PRESENT получены в результате перебора всех 16! биективных 4-битных S-блоков. Все S-блоки, найдены таким образом, что были выполнены дополнительные критерии оптимальности, и чтобы они были проанализированы с точки зрения линейной эквивалентности. Так, существует только 16 различных неэквивалентных классов [6]. Все S-блоки, члены в этих классах, являются

оптимальными S-блоками в отношении линейных и дифференциальных свойств. Эти S-блоки также оптимальны по отношению к алгебраической степени или сопротивляемости к алгебраическим атакам.

Заметим, что аналогичная работа по поиску оптимальных подстановок прямым перебором всего множества полубайтовых S-блоков выполнена в работе [7]. В ней получены S-блоки, названные золотыми. Им посвящена работа [8].

Вместо перебора всех 16! биекций из 16 элементов, как это было сделано при проектировании до настоящего времени, предлагается компактная, быстрая и элегантная методология построения криптографически сильных S-блоков с помощью квазигрупп порядка 4. Целью, которую поставили перед собой авторы работы, является дать криптографам итерационный инструмент для проектирования криптостойких S-блоков, которые обозначены ими как QS-блоки, поскольку их строительство осуществляется с помощью квазигрупп. В общем, предлагаются S-блоки, которые являются конкурентоспособными S-блоку шифра PRESENT.

Мы не будем здесь детально останавливаться на развиваемой в работе методологии, а остановимся сразу на её результатах.

В работе [3] приведено три примера «оптимальных Q-S-блоков, построенных по предлагаемому методу. Первый Q-S-блок представляет результаты применения методики (в обозначении авторов работы) с двумя лидерами и четырьмя циклами. Отмечается, что всего число таких Q-S-блоков, у которых выходные биты имеют алгебраическую степень 3, есть 128. Один из них представлен в работе, и он же приведен в третьей строке табл. 1. Авторы в [3] приводят ещё два примера построения Q-S-блоков, они также помещены в табл. 1 (строки первая и вторая).

В четвёртой строке табл. 1 представлен один из Q-S-блоков, построенных с помощью методики с четырьмя лидерами и четырьмя циклами (один лидер в каждом цикле). Число Q-S-блоков, у которых все выходные биты имеют алгебраическую степень 3, в данном случае равно 1024.

В пятой строке таблицы представлен пример ещё одного из Q-S-блоков для эксперимента с восемью лидерами и восемью циклами. Число QS-блоков, у которых все выходные биты здесь имеют алгебраическую степень 3, равно 331264.

В седьмой строке таблицы представлен S-блок шифра PRESENT, в девятой–двенадцатой строках приведены примеры золотых S-блоков из работы [7], а в двух последних строках приведены S-блок шифра DES (первая строка первого S-блока) и S-блок шифра AES (полубайтовый S-блок, построенный по идеям разработчиков шифра).

Заострим попутно внимание на формальном определении оптимального S-блока, приведенном в работе [3].

Таблица 1

Примеры S-блоков, участвующих в экспериментах

S-блоки из работы [3]																
Нулевая строка	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S_1(x)$	C	1	2	E	F	9	3	4	8	0	A	B	7	D	6	5
$S_2(x)$	D	9	F	C	B	5	7	6	3	8	E	2	0	1	4	A
$S_3(x)$	5	E	6	D	7	4	2	A	8	C	0	9	1	B	F	3
S-блок шифра PRESENT																
$S_4(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
«Золотые» S-блоки из работы [7]																
$S_5(x)$	0	3	5	8	6	9	C	7	B	A	E	4	1	F	B	2
$S_6(x)$	0	3	5	8	6	A	F	4	E	D	9	2	1	7	C	B
$S_7(x)$	0	3	5	8	6	C	B	7	9	E	A	D	F	2	1	4
$S_8(x)$	0	3	5	8	6	C	B	7	A	4	9	E	F	1	2	D
S-блоки шифров DES и AES																
$S_9(x)$	A	4	3	B	8	E	2	C	5	7	6	F	0	1	9	D
$S_{10}(x)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Определение. Пусть S будет 4×4 -битным S-блоком. Если S полностью удовлетворяет приведенным ниже условиям, мы называем S оптимальным S-блоком:

S является биекцией;

$\text{Lin}(S) = 1/4$ (максимальное значение вероятности линейной аппроксимационной таблицы S-блока);

$\text{Diff}(S) = 1/4$ (максимальное значение вероятности перехода XOR таблицы S-блока).

Все Q-S-блоки табл. 1 являются оптимальными в отмеченном смысле.

После этих кратких сведений можно приступить уже к анализу результатов выполненных оценок дифференциальных свойств шифров, использующих различные конструкции S-блоков.

2. РЕЗУЛЬТАТЫ СТАТИСТИЧЕСКИХ ЭКСПЕРИМЕНТОВ С УМЕНЬШЕННЫМИ МОДЕЛЯМИ ШИФРОВ С РАЗЛИЧНЫМИ КОНСТРУКЦИЯМИ ПОДСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ

В табл. 2 приведены результаты оценки дифференциальных показателей шифра Хейза [9] с различными S-блоками. В первой колонке при-

ведены данные о применении в шифре идеального S-блока из работы [7] (9-я строка табл. 1), во второй, третьей и четвёртой колонках представлены дифференциальные показатели (поцикловые значения максимумов полных дифференциалов) шифра Хейза, когда в нём используются S-блоки из рассматриваемой работы [3] (3–5 строки табл. 1). В остальных колонках табл. 2 в шифре используются S-блоки из шифров DES (первая строка первого S-блока) и AES («родной» S-блок) и, наконец, S-блок шифра PRESENT (7-я строка табл. 1). Во всех случаях в шифре применялись наборы из одних и тех же S-блоков.

Из представленных результатов следует, что предлагаемая в работе [3] методика позволяет получить S-блоки, отнюдь не обладающие оптимальными динамическими свойствами. Число циклов для прихода к стационарному состоянию, характерному для случайной подстановки, для всех трёх примеров оказалось превышающим семь. S-блок $S_1(x)$ выходит к асимптотическому значению лишь на одиннадцатом цикле. Такие показатели свойственны случайным S-блокам [2].

Рассматриваемые S-блоки оказались ничуть не лучше уже известных S-блоков, заметно усту-

Таблица 2

Значения максимумов полных дифференциалов для различных S-блоков и различного количества циклов алгоритма Хейза

Sbox r	Идеальный Sbox	S-box S_1	S-box S_2	S-box S_3	S-box DES	S-box AES	S-box PRESENT
1	16384	16384	16384	16384,00	32768,00	16384,00	16384,00
2	4096	4096	4096	4096,00	12288,00	4096,00	4096,00
3	512,13	2048,00	2338,67	1454,93	2303,33	2036,27	516,27
4	81,40	1132,00	631,47	404,40	222,27	596,00	61,07
5	30,40	514,07	278,00	119,53	64,13	190,33	24,93
6	19,20	229,47	113,40	43,67	24,80	77,47	18,93
7	19,07	116,93	51,53	20,60	18,80	35,87	19,40
8	19,87	59,87	27,40	19,13	18,80	21,07	18,80
9	19,07	32,13	19,07	19,07	19,00	19,27	19,27
10	19,53	20,47	19,20	19,13	18,93	19,33	19,13
11	19,13	18,73	18,47	19,20	18,93	19,00	18,93

пая по динамическим показателям идеальным S-блокам из работы [6]. Осталось засомневаться в качестве S-блоков, использованных в шифре PRESENT. Но как показывают результаты экспериментов (см. последнюю колонку табл. 2), в шифре PRESENT S-блоки, выбранные путём полного перебора, повторяют характеристики идеальных S-блоков из работы [7] (также полученных путем полного перебора всех $16!$ полубайтовых подстановок симметрической группы).

В табл. 3 приведены результаты экспериментов с уменьшенной моделью шифра Rijndael, в котором опять использованы S-блоки из табл. 2. Здесь шифр Rijndael выступает как шифр с сильным линейным преобразованием, в противовес шифру Хейза, который в наших экспериментах отражал шифр со слабым линейным преобразованием.

Из полученных результатов следует, что шифр с сильным линейным преобразованием не чувствует разницы между S-блоками. Для него все S-блоки оказались эквивалентными по динамическим показателям прихода шифра к стационарному состоянию. Предлагаемые конструкции S-блоков здесь никаких преимуществ по сравнению с другими не имеют, и S-блоки, не являющиеся в рассмотренном выше смысле оптимальными, показывают высокие результаты.

Учитывая дуальную связь дифференциальных и линейных показателей, можно сделать вывод, что аналогичные результаты будут справедливы и для линейных корпусов рассмотренных шифров (линейные и дифференциальные показатели по динамике близки друг к другу [10 и др.]).

ВЫВОДЫ

Представленные результаты экспериментов свидетельствуют, что предлагаемый в работе метод получения оптимальных S-блоков не может претендовать на оригинальность и полезность. Криптографические показатели формируемых S-блоков значительно уступают золотым (идеальным) S-блокам из работы [6] и показателям S-блоков шифра PRESENT [2]. Они практически повторяют динамические показатели S-блоков, сгенерированных случайным образом.

Для шифров с сильным линейным преобразованием поиск S-блоков с улучшенными криптографическими показателями теряет смысл. Здесь задача может быть успешно решена на

основании использования S-блоков, сгенерированных случайным образом.

С другой стороны, раз оказываются востребованными шифры со слабыми линейными преобразованиями, то задача поиска оптимальных полубайтовых S-блоков для них практически решена. В качестве таких решений могут выступать идеальные (золотые) S-блоки, найденные в работе [6]. Они с успехом применяются уже в шифрах Serpent и PRESENT. И в этом случае задача поиска оптимальных S-блоков также теряет смысл.

Нельзя не отметить ещё один важный полученный результат. Он состоит в том, что шифр PRESENT со своими S-блоками имеет весьма высокий запас прочности. Он с успехом сможет реализовать потенциальные показатели по стойкости к атакам дифференциального и линейного криптоанализа и при числе циклов зашифрования более чем вдвое меньшем заявленного в разработке, если учитывать и сопротивляемость шифра к бумеранг атаке, требующей от шифра обеспечения стойкости на половине его цикловой длины.

Литература

- [1] *Lisitskaya I.V.* Importance of S-Blocks in Modern Block Ciphers. / I.V. Lisitskaya, E.D. Melnichuk and K.E. Lysytskiy. // I.J. Computer Network and Information Security – 2012. – 10 – С. 1–12.
- [2] *Лисицкая И.В.* Методология оценки стойкости блочных симметричных шифров. / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123–133.
- [3] *Hristina Mihajloska*, Skopje, Macedonia, Danilo Gligoroski Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4 SECURWARE 2012 : The Sixth International Conference on Emerging Security Information, Systems and Technologies pp. 163–168.
- [4] *A. Bogdanov, L. R. Knudsen, G. Le, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Viskelsoe*, “PRESENT: An Ultra-Lightweight Block Cipher,” in The Proceedings of CHES 2007. Springer-Verlag, 2007. – P. 450–466.
- [5] *T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel*, “A Survey of Lightweight-Cryptography Implementations,” in IEEE Design and Test, vol. 24, no. 6. IEEE Computer Society Press, November, 2007. – P. 522–533.
- [6] *G. Leander and A. Poschmann*, “On the Classification of 4 Bit S-Boxes,” in Proceedings of the 1st International Workshop on Arithmetic of Finite Fields. Springer-Verlag, 2007. – P. 159–176.

Таблица 3

Значения максимумов полных дифференциалов для различных S-блоков и количества циклов алгоритма Rijndael. Линейная часть – MixColumn GF(2⁴) и ShiftRow.

S-box г	S-box идеальный	S-box S ₁	S-box S ₂	S-box S ₃	S-box PRESENT	S-box DES	S-box AES	Случайный S-box
1	16384	16384,00	16384,00	16384,00	16384,00	32768,00	16384,00	49152,00
2	3054,93	3413,33	3106,13	3037,87	3089,07	1152,00	3072,00	5184,00
3	381,60	353,07	290,13	340,27	314,67	70,87	272,00	146,13
4	19,53	19,53	19,40	19,33	19,33	19,27	19,20	19,07
5	18,93	19,20	19,13	19,13	19,20	19,00	19,27	19,00
6	19,07	19,07	19,13	19,20	18,47	19,00	19,13	19,00

- [7] *Markku-Juhani O. Saarinen*: Cryptographic Analysis of All 4 x 4 - Bit S-Boxes, In SAC 2011, August 2011 Toronto, Canada, Springer LNCS. A version is available at eprint.iacr.org/2011/218/
- [8] *Кобылина Ю.И.* Дифференциальные свойства малых версий современных шифров при использовании в них идеальных подстановок / Ю.И. Кобылина, К.Е. Лисицкий // Сборник трудов Второй Международной научно-технической конференции «Компьютерные науки и технологии» 3-5 октября. — Белгород. — 2011. — С. 423–425.
- [9] *H. M. Heys*. A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002. — P. 189–221.
- [10] *Лисицька І.В.* Большие шифры — случайные подстановки. Сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс и их уменьшенных моделей / І.В. Лисицька, А.А. Настенко, К.Є. Лисицкий // Автоматизовані системи управління та прибори автоматики. — 2012. — Т. 159. №. — С. 31–39.

Поступила в редколлегию 27.06.2014



Лисицкий Константин Евгеньевич, магистр Харьковского национального университета им. В.Н. Каразина. Научные интересы: технологии блочного симметричного шифрования.

УДК 621. 391:519.2:519.7

Знову про оптимальні S-блоки / К.Є. Лисицкий // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 208–212.

Наводяться результати оцінки динамічних показників процесу приходу шифру Хейза і зменшеної моделі шифру Rijndael за диференціальними показниками до стаціонарних станів, властивих випадковим підстановкам в ході використання в шифрах напівбайтових підстановок, сконструйованих різними способами. Показано, що запропонований в одній з останніх публікацій метод формування оптимальних QS-блоків з використанням квазігруп насправді не призводить до підстановок з поліпшеними криптографічними показниками. Робиться висновок, що пошук напівбайтових S-блоків з поліпшеними властивостями втратив сенс. Кращі підстановлювальні перетворення вже отримано на основі повного перебору всієї множини напівбайтових підстановок симетричної групи.

Ключові слова: підстановка, оптимальний S-блок, динамічні показники шифру, максимуми повних диференціалів.

Табл.: 3. Бібліогр.: 10 найм.

UDC 621. 391: 519. 2: 519.7

Again on optimum S-boxes / К.Е. Lisitsky // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 208–212.

The paper presents the results of evaluating the dynamic performance of the Heys cipher coming process and cipher Rijndael reduced model by differential performance to steady states typical of random substitutions in using ciphers nibble substitutions engineered in various ways. It is shown that the method of forming optimum QS-blocks with the use of quasi-groups, which was suggested in one of recent publications, do not actually lead to substitutions with improved cryptographic parameters. A conclusion is drawn that searching nibble S-units with improved properties has become pointless. The best wildcard transformations have already been obtained on the basis of an complete exhaustion of the whole set of nibble substitutions of a symmetric group.

Keywords: substitution, optimal S-box, dynamic cipher performance, maxima of total differentials.

Tab.: 3. Ref.: 10 items.

УТОЧНЁННЫЕ ПОКАЗАТЕЛИ ПРИХОДА ШИФРОВ К СОСТОЯНИЮ СЛУЧАЙНОЙ ПОДСТАНОВКИ

И.Д. ГОРБЕНКО, В.И. ДОЛГОВ, К.Е. ЛИСИЦКИЙ

Представляются уточнённые данные по оценке динамических показателей перехода современных шифров к состоянию случайной подстановки за счёт учёта маловероятных активизаций входов.

Ключевые слова: подстановка, активный S-блок, состояние случайной подстановки, динамические показатели шифров.

ВВЕДЕНИЕ

В наших работах по изучению динамических показателей прихода шифров к состоянию случайной подстановки [1–3], мы искали минимальное число активных S-блоков, позволяющих осуществить этот переход. Анализ, однако, показал, что существует возможность активизации меньшего числа S-блоков, чем рассмотрено в работах [1–3]. Мы сосредоточили внимание в наших работах на наиболее вероятных переходах. В то же время существуют пускai даже маловероятные переходы, но, как оказалось, они позволяют шифрам прийти к случайной подстановке при большем числе циклов, чем те, которые были определены при использовании наиболее вероятных переходов. Они, конечно, должны быть учтены при оценке динамических показателей шифров.

В этой работе мы приводим дополнительные обоснования по оценке минимального числа циклов, после которых шифры приходят к состоянию случайной подстановки.

1. ПРИХОД ШИФРОВ К СОСТОЯНИЮ СЛУЧАЙНОЙ ПОДСТАНОВКИ ПРИ МАЛОВЕРОЯТНЫХ АКТИВИЗАЦИЯХ ВХОДОВ

Мы начнём с лидера среди современных блочных симметричных шифров алгоритма Rijndael.

При оценке динамических свойств прихода к состоянию случайной подстановки шифра Rijndael в [1–3] мы определяли минимальное число S-блоков на первом цикле преобразования этого шифра в виде одного байта, позволявшего активизировать один S-блок первого цикла. В последующем после МДР преобразования (MixColumns), использованного при построении цикловой функции этого шифра, активизировалось сразу четыре S-блока, т.е. на два цикла приходилось пять активизированных S-блоков. Однако эти же пять S-блоков можно активизировать, используя не один активный байт входа, а сразу четыре. Как показано в [4], МДР преобразование позволяет при четырёх активных байтах входа получить на выходе с вероятностью $2^{-23,983}$ один активный байт. Тогда эти четыре байта будут делать активными все четыре S-блока первого

цикла, которые за счёт МДР преобразования первого цикла (с коэффициентом ветвления 5) хоть и с весьма малой вероятностью будут активизировать только один S-блок второго цикла, так что на два цикла и в этом случае будет приходиться пять активных S-блоков. Тогда в первом случае четыре активных S-блока второго цикла с учетом преобразования ShiftRow и MixColumns, будут уже активизировать в следующем третьем цикле все шестнадцать его S-блоков (ShiftRow расставляет выходы S-блоков по одному в каждой колонке). В результате на трёх циклах, как и указывалось в наших работах, становится активным $1 + 4 + 16 = 21$ S-блок. В это же время во втором случае в третьем цикле будет активизироваться (за счёт МДР преобразования с коэффициентом ветвления 5) только четыре S-блока третьего цикла. Получается, что во втором случае число активизируемых S-блоков меньше, чем при активизации одного входного байта (в этом случае получаем $4 + 1 + 4 = 9$ S-блоков), а на четырёх циклах число активных S-блоков будет 25. В результате шифр приходит к состоянию случайной подстановки и по дифференциальным и по линейным показателям за четыре цикла, а не за три, как указано в работе [3]. Именно четыре цикла прихода шифра Rijndael к состоянию случайной подстановки определяют и сами разработчики шифра [5].

Шифр Калина-128. В этом случае необходимо было рассмотреть и активизацию входа шифра сразу восемью байтами. Тогда на первом цикле имеем восемь активных S-блоков, на втором — один (вероятность перехода восьми активных входов операции MixColumns в одноблочный активный выход равна $2^{-55,9}$ [4]), на третьем ещё восемь, на четвёртом — все шестнадцать. Шифр для этой ситуации приходит гарантировано к случайной подстановке как по дифференциальным, так и по линейным показателям тоже за четыре цикла ($8 + 1 + 8 + 16 = 33$).

Шифр FOX-64. Здесь, как отмечено в [3], функция f32 внутреннего уровня включает в себя два слоя из четвёрок байтовых S-блоков с промежуточной рассеивающей частью, представляющей собой линейную 4×4 -мультиперестановку в поле $GF(2^8)$, и три промежуточных сложения с цикловыми подключами [13]. В результате в

первом цикле активизируется минимум пять S-блоков (один S-блок первого слоя и четыре второго или четыре S-блока первого слоя и один второго).

Далее в первом случае продолжением может быть снова пять S-блоков (вероятность двух переходов в один цикл получается равной $2^{-47,966}$), так что в этом случае имеем $5 + 5 + 5 = 15$ активных S-блоков на три цикла.

Во втором случае вероятность на трёх циклах получить третий переход в один активный S-блок уже равна $2^{-71,949}$ — это уже невероятное событие). Но зато хоть и с малой вероятностью возможны переходы в два и более активных S-блоков, так что здесь имеем на три цикла $5 + 5 + 6 = 16$ активных S-блоков.

Если считать, что внешний уровень конструкции шифра (схема Лэя Мэсси) позволяет удвоить результат для активных S-блоков (для трёх циклов имеем минимум 30 активных S-блоков), приходим к выводу, что для прихода шифра Шифр FOX-64 к случайной подстановке достаточно трёх циклов и по дифференциальным и по линейным показателям: $2^{58} = 2^{-4k}$ и, следовательно, $k_{\min} = 14,5$ (2^{-4} — показатель δ -равномерности S-блоков шифра FOX [10]); $2^{58} = 2^{k-1} (2^{-4})^k$ имеем $k_{\min} = 19,3$ (2^{-4} — показатель нелинейности S-блоков шифра FOX [10]).

Шифр FOX-128. В 128-битном шифре FOX в функции f64 внутреннего уровня применяется матричное умножение на МДР матрицу 8×8 и опять двухслойное нелинейное преобразование. Поэтому на первом цикле имеем девять активных S-блоков ($1 + 8$ или $8 + 1$). На втором цикле и в первом и во втором случае будет снова девять активных S-блоков (вероятность перехода в МДР преобразовании восьми активных байтов входа в один, как и в Калине, здесь равна $2^{-55,9}$, а дважды такое событие может произойти с вероятностью $2^{-111,8}$). На третьем цикле в первом случае имеем снова девять активных S-блоков (ещё один переход $1 \rightarrow 8$), а во втором — переход $8 \rightarrow 1$ уже невероятен, и здесь можно ожидать, скорее всего, в МДР преобразовании переходы в четыре и более активных байтов. Итак, на трёх циклах минимальным числом S-блоков будет $9 + 9 + 9 = 27$, и, следовательно, в этом случае с учётом удвоения за счёт преобразования внешнего уровня на двух циклах имеем 54-е активных S-блока. Здесь $2^{120} = 2^{-4k}$ и $k_{\min} = 30$; $2^{120} = 2^{k-1} (2^{-4})^k$ и $k_{\min} = 40$. Следовательно, для шифра FOX-128 $r_{\min} = 3$ и по дифференциальным и по линейным показателям.

Шифр Мухомор-128. Конструкция функции усложнения М-64 шифра Мухомор-128 содержит три SL преобразования, в каждое из которых входит слой нелинейных преобразований, реализуемый с помощью 4-байтовых S-блоков, и МДР преобразование, осуществляющее матричное умножение байтовых выходов четырех S-блоков (над полем) на квадратную матрицу, размера 4×4 (аналогичное преобразование вы-

полняется в шифре Rijndael с помощью операции MixColumns, только там при умножении используется другой полином). На входе функции усложнения М-64 выполняется сложение 32-битных блоков данных по модулю 2^{32} . В предыдущей работе [3] отмечалось, что схема включения SL преобразований обеспечивает активизацию всех двенадцати S-блоков цикловой функции. Однако это не так. Все 12 S-блоков активизируются первым активным байтом или 4-байтовым сегментом, поступающим на вход левого первого по порядку следования SL преобразования. Но, если рассматривать ситуацию, когда активизируется второе по порядку SL преобразование, то один или более активных байтов, поступающих на вход этого SL преобразования активизируют от одного до четырёх его S-блоков, а также третье SL преобразование (первое по порядку прохождения преобразований SL преобразование не активизируется).

Если активизируются четыре байта на входе самого правого (второго по порядку прохождения) SL преобразования, то в этом SL преобразовании активизируются четыре S-блока, которые после МДР преобразования дают один активный байт и, следовательно, в третьем (по порядку прохождения) SL преобразовании активизируется один S-блок. Этот один S-блок формирует четыре активных байта левого 32-битного выходного блока данных цикловой функции, и они же, складываясь с одноблочным выходом правого SL преобразования, формируют четыре активных байта правого 32-битного выходного блока данных цикловой функции. Получается, что в формировании выхода левого полублока цикловой функции принимают участие пять S-блоков, а в формировании правого полублока цикловой функции принимают участие шесть S-блоков.

В результате для прихода к случайной подстановке функции усложнения М-64 одного цикла не хватает.

Второй цикл в рассматриваемом случае позволяет активизировать SL преобразования второго цикла по схеме $1 + 4 + 2$ активных S-блока (можно ориентироваться на два маловероятных перехода МДР преобразований), что для левого и правого полублоков цикловой функции второго цикла даёт семь активных S-блоков. На два цикла в рассматриваемом случае приходится минимум двенадцать активных S-блоков. Это два цикла прихода к состоянию случайной подстановки по дифференциальным показателям и три по линейным.

Если опять удваивать результат прохождения функции усложнения М-64 для того, чтобы оценить число активных S-блоков для всей цикловой функции шифра Мухомор, то приходим к результату: для одного цикла — 10 S-блоков, для двух циклов — 24 S-блока.

Для шифра Мухомор: $2^{-120} = 2^{-5k}$ и $k_{\min} = 24$; $2^{-120} = 2^{k-1} (2^{-5})^k$ и $k_{\min} = 30$ (2^{-5} — показатель

δ -равномерности и показатель нелинейности S-блоков шифра Мухомор). Это означает, что шифр Мухомор-128 приходит к случайной подстановке по линейным показателям за три цикла ($r_{\min} = 3$).

Шифр Мухомор-256. Конструкция функции усложнения М-128 шифра Мухомор-256 (вход в шифр 256 битов) состоит из восьми SL преобразований [16].

Опять рассмотрим активизацию самого правого 4-байтового блока данных, поступающих на правое SL преобразования первой линейки SL преобразований. Сразу рассмотрим все четыре байта входа этого SL преобразования активными. Как и в предыдущем случае имеем все четыре S-блока этого преобразования активными. На выходе SL преобразования один активный байт. В результате этот активный байт активизирует один S-блок первого SL преобразования второй линейки SL преобразований и далее идёт цепочка $4 \rightarrow 1 + 4 \rightarrow 4$ (событие более двух переходов $4 \rightarrow 1$, или второй переход $4 \rightarrow 1$ или второй переход $4 \rightarrow 3$ это практически невозможные события). Это, если не учитывать дополнительных обратных связей. Дополнительные обратные связи позволяют для первого 32-битного выхода получить оценку для числа активных S-блоков, участвующих в его формировании в виде $4 + 1 + 4 + 4 + 4 = 17$. Для второго 32-битного блока — $4 + 1 + 4 + 9 + 13 = 31$ и т.д. Минимальным значением является 17. С учётом удвоения (за счёт преобразований внешнего уровня) получается 34 S-блока. Будем считать, что второй цикл даёт 33 активных S-блока, а с учётом удвоения — 66 активных S-блоков.

Для шифра Мухомор-256: $2^{-248} = 2^{-5k}$ и $k_{\min} = 49,6$; $2^{-248} = 2^{k-1} (2^{-5})^k$ и $k_{\min} = 62$ (2^{-5} — показатель δ -равномерности и показатель нелинейности S-блоков шифра Мухомор).

В результате шифр будет выходить к показателям случайной подстановки за два цикла и с показателями δ -равномерности равным 8-ми, 10-ти, 12-ти, 16-ти и даже 20-ти (при $\delta = 16$ минимально необходимое число S-блоков есть 30).

Белорусский шифр имеет в цикловой функции 28 блоков, из которых активизируется на первом цикле минимум 10–18 S-блоков, и, как отмечено в [3], шифр приходит к состоянию случайной подстановки за два цикла.

С данными по остальным шифрам можно согласиться.

2. СВОДКА УТОЧНЁННЫХ РЕЗУЛЬТАТОВ

С учетом уточнённых данных мы теперь снова приведём сводку полученных результатов. Она оформлена в виде табл. 1 и табл. 2.

Практически изменения коснулись только шифров Rijndael, Калина, и функций усложнения шифров Мухомор-128 и Мухомор-256. Новые данные отличаются от старых увеличением числа циклов выхода шифров к состоя-

нию случайной подстановки на один цикл. Для нас важно, что известные современные шифры, претендующие на лидерство, как, оказалось, требуют для выхода к случайной подстановке трёх и более циклов.

Таблица 1

Минимальное число циклов для выхода шифра по дифференциальным показателям к стационарному состоянию случайной подстановки

Шифр	$r_{\min}$
Rijndael-128	4
Калина-128	4
FOX-64	3
FOX-128	3
ГОСТ 28147-89	9
Мухомор-128	2
Мухомор-256	2
Serpent	3
Лабиринт	i
Шифр с цикловой функцией М-64	2
Шифр с цикловой функцией М-128	2

Таблица 2

Минимальное число циклов для выхода шифра по линейным показателям к стационарному состоянию случайной подстановки

Шифр	$r_{\min}$
Rijndael-128	4
Калина-128	4
FOX-64	3
FOX-128	3
ГОСТ 28147-89	9
Мухомор-128	3
Белорусский шифр	2
Serpent	3
Лабиринт	i
Шифр с цикловой функцией М-64	2
Шифр с цикловой функцией М-128	2

ВЫВОДЫ

Общим выводом можно отметить, что все известные современные шифры имеют число циклов выхода к состоянию случайной подстановки 3 и более.

Как показывает анализ, все известные конструкции цикловых функций не ориентированы на активизацию всех S-блоков первого цикла.

Отдельно можно выделить блочный шифр из белорусского стандарта и разработки шифров Мухомор. Они позволяют по нашим данным осуществить переход к состоянию случайной подстановки за два цикла.

Возникает интересный вопрос. А можно ли построить шифр, который становился бы случайной подстановкой уже с первого цикла? Чего это будет стоить? По видимому, нужно строить первый цикл не привязываясь к подобию всех цикловых преобразований. Мы на него постараемся ответить в нашей следующей работе.

Литература

- [1] *Gorbenko I.D., Lisitskiy K.E., Denisov D.S.* (2014). On Ciphers Coming to a Stationary State of Random Substitution. *Universal Journal of Electrical and Electronic Engineering*, 2, 206–215. doi: 10.13189/ujeee.2014.020409.
- [2] *Горбенко И.Д.* О динамике прихода блочных симметричных шифров к случайной подстановке / И.Д. Горбенко, Е.К. Лисицкий // Радиотехника. Всеукр. межвед. научн.-техн. сб. — 2014. — Вип.176. — С. 27–39.
- [3] *Лисицкий К.Е.* Динамические показатели прихода блочных шифров к состоянию случайной подстановки / К.Е. Лисицкий // Издательский дом LAP LAMBERT Academic Publishing, 2014. — 60 с.
- [4] *Руженцев В.И.* О методе доказательства стойкости блочных шифров к атаке невыполнимых дифференциалов / В.И. Руженцев // Прикладная радиоэлектроника. — 2013. — Т. 12. — № 2. — С. 215–219.
- [5] *J. Daemen and V. Rijmen.* AES Proposal: Rijndael. 1st AES Conference, California, USA, 1998. <http://www.nist.gov/aes>.

Поступила в редколлегию 8.07.2014

Горбенко Иван Дмитриевич, профессор кафедры безопасности информационных систем и технологий Харьковского национального университета имени В.Н. Каразина, Главный конструктор ПАТ «ИИТ». Научные интересы: криптографические системы и протоколы, проектирование и разработка систем, комплексов и средств криптографической защиты информации.



Долгов Виктор Иванович, профессор кафедры безопасности информационных систем и технологий Харьковского национального университета имени В.Н. Каразина. Научные интересы: методы криптоанализа, технологии блочного симметричного шифрования.

Лисицкий Константин Евгеньевич, фото и сведения об авторе см. на с. 212.

УДК 621.391:519.2:519.7

Уточнені показники приходу шифрів до стану випадкової підстановки / І.Д. Горбенко, В.І. Долгов, К.Є. Лисицкий // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 213–216.

Надано уточнені дані щодо оцінки динамічних показників переходу сучасних шифрів до стану випадкової підстановки за рахунок обліку малоімовірних активізацій входів.

Ключові слова: підстановка, активний S-блок, стан випадкової підстановки, динамічні показники шифрів. Табл.: 2. Бібліогр. 5 найм.

UDC 621.391:519.2:519.7

Ascertained indicators of ciphers coming to the state of random substitution / I.D. Gorbenko, V.I. Dolgov, K.E. Lisitskiy // *Applied Radio Electronics: Sci. Journ.* — 2014. — Vol. 13. — № 3. — P. 213–216.

The paper presents ascertained data on the evaluation of dynamic indicators of the transition of present-day ciphers to the state of random substitution with due account of unlikely input activation.

Keywords: substitution, active S-box, state of random substitution, dynamic indicators of ciphers.

Tab.: 2. Ref.: 5 items.

ДОСЛІДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЕРСПЕКТИВНИХ ПОТОКОВИХ ШИФРІВ

С.С. ТИМОХІН, І.Д. ГОРБЕНКО

Потокові симетричні шифри відіграють важливу роль для захисту інформації, для якої висуваються значні вимоги до рівня стійкості та швидкості обробки в режимі он-лайн. Апаратно орієнтовані потокові шифри мають забезпечувати достатній рівень стійкості, швидкодії та бути компактними при апаратній реалізації. Нелінійні регістри зсуву є одним з підходів побудови апаратних шифрів, що є на сьогодні мало дослідженим і вимагає уваги.

Ключові слова: потокове шифрування, нелінійні регістри зсуву.

ВСТУП

Симетричні криптографічні примітиви шифрування поділяються на потокові та блокові шифри. Основні принципи побудови та аналізу безпеки блокових симетричних шифрів (БСШ) є добре вивченими та дослідженими, на відміну від поточкових симетричних шифрів (ПСШ). Теоретично, БСШ можуть надійно виступати як потоковий шифр (генерування гами) у режимі OFB та CFB [3], тому виникає питання про доцільність розробки, вивчення та дослідження методів побудови, оцінки безпеки та аналізу ПСШ. Практично ж, потокові симетричні шифри використовуються у тих випадках, де використання класичних блокових шифрів є неефективним. Наприклад, у режимі реального часу, коли швидкість роботи системи є одним з основних критеріїв її ефективності. У такому випадку, спеціально розроблені ПСШ працюють набагато швидше, ніж БСШ у режимах OFB та CFB. Тому, під час розробки таких шифрів, до них висувають жорсткі вимоги щодо швидкодії при програмній реалізації та розміру (а, відповідно, і вартості).

Найбільшим поштовхом для розвитку ПСШ був проект eSTREAM (2004 – 2008 рр.), після того, як були знайдені уразливості в актуальних ПСШ (наприклад, SNOW). Метою цього проекту була розробка швидких та ефективних програмних шифрів і невеликих та надійних апаратних шифрів. На сайті проекту можна знайти роботи, присвячені ПСШ, що проходили відбір з двох критеріями: програмні та апаратні шифри. Кращими програмними шифрами було обрано HC, Rabbit, Salsa, Sosemanuk та кращими апаратними шифрами було обрано Grain, Trivium та Mickey.

1. СТИСЛІ ВІДОМОСТІ ПРО ПОТОКОВІ ШИФРИ

Відомо, що шифром з абсолютною стійкістю є шифр Вернама (One-time Pad). Недоліком цього шифру є те, що довжина ключа має бути не меншою, ніж довжина повідомлення. Зберігати такий ключ дуже важко, тому інженери намагаються розробити деякий генератор гами, що відповідав би певним вимогам, та розгортав би з невеликого ключа та вектора ініціалізації досить

велику псевдовипадкову послідовність. Шифр Вернама можна записати у вигляді (1)

$$E : \{0,1\} \times \{0,1\} \rightarrow \{0,1\}, (m, k) \rightarrow m \oplus k, \quad (1)$$

де m та k є відкритий текст та ключовий потік відповідно. Процедури шифрування (2) та розшифрування (3) можна записати у вигляді

$$E_{k_i}(m_i) = m_i \oplus k_i = c_i, \quad (2)$$

$$D_{k_i}(m_i) = c_i \oplus k_i = m_i. \quad (3)$$

ПСШ генерує n -бітову послідовність, базуючись на внутрішньому стані генератора. Техніка генерування гами може бути різною, деякі реалізації можуть ефективно працювати на 8-, 16-, 32- або 64-бітових архітектурах, або навіть за умови певної особливої апаратної реалізації.

Вимоги. Ключовий потік, тобто гама, що генерується, генератор псевдовипадкових чисел має задовольняти такі вимоги [1]:

1. Мати заданий період, тобто $l_G \geq l_d$, де l_d є мінімальне допустиме значення періоду.
2. Гама повинна мати складний закон її формування, інакше вона може бути визначена під час криптоаналізу.
3. Відновлюваність гами у часі і просторі, тобто можливість її точного відтворення.
4. Мінімальна або сприйнятна складність реалізації функції генерації гами.
5. Допустима величина перекриття шифруючої гами, під якою розуміють імовірність з'явлення однієї і тієї ж гами в просторі або часі, як на одній, так і у різних станціях.

Швидкість. Швидкодія шифрів (генерація гами) обчислювалась на комп'ютері з процесором Intel Core i7-3630QM з тактовою частотою 2.4 ГГц. Код написаний C++ та скомпільований за допомогою компілятора MinGW gcc-g++ версії 4.8.1-4. У таблиці не наводиться швидкодія апаратно орієнтованих шифрів, оскільки їх програмна модель є дуже повільною 2–13 Мбіт/с. Оцінка швидкодії даних шифрів є доречною за наявності апаратної реалізації.

Безпека. Усі шифри, що проходили відбір під час проекту eSTREAM, потрапили під детальний аналіз та дослідження. Деякі шифри були взламні ще під час проекту, але помилки були

Порівняння параметрів та швидкодії програмно орієнтованих шифрів

Назва шифру	Розмір ключа (біт)	Розмір вектора ініціалізації (біт)	Швидкодія генерування (Мбіт/с)	Швидкодія процесу ініціалізації (мкс)
HC128	128	128 біт	2521	16,9
Rabbit	128	64	1764	1,7
Salsa20	128	64	2006	0,8
Sosemanuk	256	128	1610	15,8

виправлені та випущені нові версії шифрів. Так, наприклад, початкова версія апаратно орієнтованого шифру Grain мала уразливість, що давала можливість здійснити атаку та розкрити секретний ключ зі складністю 2^{40} [7].

Станом на сьогодні, багато шифрів залишаються стійкими та не існує атаки зі складністю, меншою за повний перебір ключа. Такі програмні шифри, як HC, Rabbit, Sosemanuk, Salsa20/7 та вище, апаратні шифри Grain, Mickey, Trivium залишаються надійними та рекомендованими до використання.

2. НЕЛІНІЙНІ РЕГІСТРИ ЗСУВУ

Одним з перспективних і мало досліджених методів побудови апаратних генераторів псевдовипадкових послідовностей є використання нелінійних регістрів зсуву зі зворотним зв'язком (NLFSR). NLFSR є узагальненням лінійного регістру зсуву зі зворотним зв'язком (FLSR), у яких поточний стан є нелінійною функцією від попереднього стану. Така зацікавленість NLFSR викликана тим, що вони спроможні генерувати великі псевдовипадкові послідовності, що будуть важко розкриті, використовуючи існуючі методи криптоаналізу. Відомо [1], що для того, щоб виявити функцію зворотного зв'язку для LFSR методом Берлекемпа-Мессі, необхідно перехопити лише $2n$ бітів послідовності. Для того, щоб заплутати криптоаналітика, були розроблені алгоритми для підвищення лінійної складності послідовностей: наприклад, використання проріджувачів генераторів, нелінійні комбінації NLFSR або нелінійні фільтри [4].

Брюс Шнайер ще у 1994 році [5] писав, що нелінійні регістри зсуву є дуже цікавими з точки зору побудови поточних симетричних шифрів, але вони не мають достатнього математичного апарату для описання та аналізу. Для послідовностей, що генеруються за допомогою NLFSR, є характерні такі проблеми:

— у вихідній послідовності можуть бути зсуви, наприклад, одиниць більше ніж нулів;

— максимальний період може бути менший ніж очікувалось;

— період для різних початкових станів може бути різним;

— послідовність може деякий час виглядати як випадкова, а потім зводиться до якого-небудь єдиного значення.

На сьогоднішній день нелінійні регістри зсуву використовуються у декількох алгоритмах потокового шифрування, таких як Achterbahn, Grain, Trivium [4], причому останні є фіналістами eSTREAM. Але навіть ці NLFSR не є ідеальними. Розглянемо NLFSR потокового шифру Grain [3]. Оскільки у попередній версії шифру була виявлена атака, яка дозволяла знайти секретний ключ за $O(2^{40})$, виявивши лінійну функцію, що могла з ймовірністю більшою за S передбачити наступний біт. Для посилення стійкості шифру, автори змінили нелінійну функцію зворотного зв'язку, що на сьогоднішній день використовує 13 бітів 80-бітового регістру та має рівень нелінійності 11. Якщо заповнити його тільки одиницями, тоді він починає генерувати 0 і ніколи не виходить з цього стану. Тобто, він зводиться до певного єдиного значення. Зазвичай, конструкція шифру включає в себе лінійний регістр, що подає на вхід NLFSR свій молодший біт і дозволяє вивести регістр із-за циклювання. Таким чином, важливим є пошук методу побудови нелінійного регістру зсуву, що не мав би в собі вищезазначених вад. Тобто, для побудови NLFSR висуваються такі вимоги:

— рівномірність розподілу вихідних значень;

— генерація послідовності максимальної довжини (послідовність де Бруїна);

— відсутність підциклів;

— відсутність зациклювань.

На цю тему проводилося дуже багато досліджень [2, 4, 6, 7]. У роботі [7] був запропонований метод, що дозволяє побудувати нелінійний регістр зсуву зі зворотним зв'язком, що генеруватиме послідовність максимальної довжини. На рис. 1 показана узагальнена структура регістру зсуву

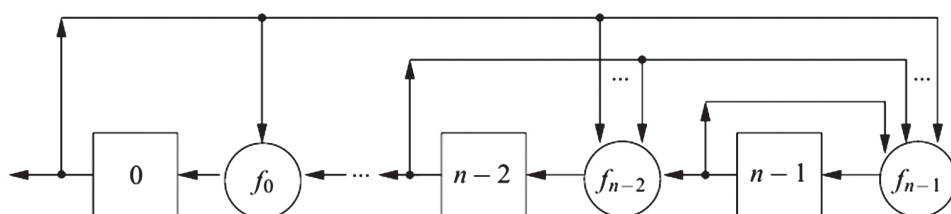


Рис. 1. Узагальнена структура регістру зсуву

Таблиця 3

Послідовності, побудовані за допомогою нелінійних та лінійних регістрів зсуву

Регістр	Послідовність
LFSR	0b0011010111100010
NLFSR	0b0001001101011110

З таблиці можна помітити, що це є одна і та сама послідовність, тільки зсунута одна відносно одної. Саме це стало причиною того, що послідовність не проходить тест NIST, адже існує лінійний поліном, за допомогою якого можна побудувати дану послідовність.

ВИСНОВКИ

Таким чином, основним вибором критеріїв ефективності потокового шифру є їх швидкодія, час генерування гами та ініціалізації. Вищезгадані шифри є надійними з точки зору безпеки і ефективними з точки зору швидкодії. Тим не менш, продовжується активне дослідження потокових шифрів, пошук ефективних способів і методів побудови шифрів та їх аналізу. Привабливими з точки зору криптоаналізу є шифри HC, адже він є подібним до RC4, який на сьогоднішній день є зламаним, шифр Trivium є дуже простим, на перший погляд, але тим не менш, жодної ефективної атаки на нього зроблено не було.

Найбільш цікавим з точки зору дослідження, на мою думку, є шифр Grain, адже він має у своєму складі нелінійний регістр зсуву, для яких досі не існує математичних методів оцінки та дослідження їх властивостей.

Питання побудови достатньо ефективного та надійного нелінійного регістру зсуву зі зворотним зв'язком досі залишається відкритим. Генератори, побудовані за допомогою вищезазначеної теореми є поштовхом для дослідження та побудови їх властивостей, але їх ще зарано використовувати в ході побудови сучасних потокових шифрів. Задача стоїть у необхідності знаходження функції нелінійного зворотного зв'язку, тоді до неї необхідно висунути певні вимоги, задовольняючи які, послідовність би мала необхідну лінійну складність.

Література

- [1] Горбенко І.Д. Прикладна криптологія: теорія, практика, застосування. — Х.: Форт, 2012. — 867 с.
- [2] A statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (NIST 800-22) — Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, 2010. — 131 p.

Таблиця 2

Результати тестування послідовностей за допомогою NIST 800-22

Поліноми \ k	3							10						
	C ₀	C ₁	C ₂	C ₃	C ₄	C ₅	C ₆	C ₀	C ₁	C ₂	C ₃	C ₄	C ₅	C ₆
(46, 5, 3, 2, 1, 0)	2000	0	0	0	0	0	0	2000	0	0	0	0	0	0
(47, 5, 0)	2000	0	0	0	0	0	0	2000	0	0	0	0	0	0
(66, 9, 8, 6, 0)	2000	0	0	0	0	0	0	2000	0	0	0	0	0	0

зсуву, де $0 \dots n-1$ є поточним станом регістру зсуву, а f_i є функцією оновлення значення i . Існує теорема, що дозволяє побудувати нелінійний регістр зсуву, використовуючи простий незвідний поліном.

Теорема. Нехай N є нелінійний регістр зсуву розміру n та функції зворотного зв'язку задані у вигляді:

$$\begin{aligned} f_{n-1}(x_0, x_1, \dots, x_{n-2}) &= \\ &= x_0 + f_L(x_0, x_1, \dots, x_{n-2}) + f_N(x_0, x_1, \dots, x_{n-2}) \\ f_{n-2}(x_0, x_1, \dots, x_{n-3}, x_{n-1}) &= x_{n-1} + f_N(x_0, x_1, \dots, x_{n-3}) \\ f_{n-3}(x_{n-2}) &= x_{n-2} \\ &\dots \\ f_0(x_1) &= x_1, \end{aligned} \quad (4)$$

де f_N є довільною нелінійною функцією, а f_L — лінійною булевою функцією виду (5), що побудована за допомогою простого незвідного полінома, тоді регістр має період $2^n - 1$.

$$f_L(x_1, x_2, \dots, x_{n-2}) = c_1 x_1 + c_2 x_2 + \dots + c_{n-2} x_{n-2}. \quad (5)$$

Доведення цієї теореми можна знайти у роботі [7]. Була проведена робота з дослідження цього методу генерації нелінійних регістрів зсуву. Дійсно, згенерована послідовність має максимальний період. Для тестування обирались незвідні поліноми різної довжини, як нелінійна функція була обрана функція виду:

$$\begin{aligned} f_N(x_0, x_1, \dots, x_k) &= x_0 x_1 + x_0 x_2 + \dots + x_0 x_k + x_1 x_2 + \dots + \\ &+ x_{k-1} x_k + x_0 x_1 x_2 + \dots + x_0 x_1 \dots x_k, \end{aligned} \quad (6)$$

де k змінювалося у межах [2, 25].

Будувалися послідовності, які потім тестувалися за допомогою стандарту NIST 800-22 [2]. Дані послідовності проходили усі тести, окрім тесту на лінійну складність. У табл. 2 наведено результати тестування послідовностей, що генерувалися за допомогою даної методики. Параметри тесту обирались стандартними.

З даної таблиці видно, що дані послідовності не мають достатньої лінійної складності, адже розподіл параметра S повністю сконцентрований у першому інтервалі і не відповідає необхідному розподілу ймовірностей. Іншими словами, дана послідовність не є достатньо складною для використання. Причиною тому є те, що даний генератор генерує ту ж саму лінійну послідовність, що й LFSR. Наприклад, у табл. 3 наведено дві послідовності, згенеровані за допомогою LFSR та NLFSR, побудовані за допомогою полінома (4, 1, 0) та функції нелінійного зсуву (7).

$$f_N = x_1 x_2 + x_1 x_3 + x_2 x_3 + x_1 x_2 x_3. \quad (7)$$

- [3] A Stream Cipher for Constrained Environments / Martin Hell, Thomas Johansson and Willi Meier // eStream. — 2008. — P. 14. — Режим доступа: <http://cr.yp.to/streamciphers/grain/desc.pdf>
- [4] Mattsson J. Stream Cipher Design — Stockholm: Master of Science Thesis, 2006. — 62 p.
- [5] Шнайер Б. Прикладная криптология. М.: Диалектика, 1994. — 432 с.
- [6] A Scalable Method for Constructing Galois NLFSRs with Period $2^n - 1$ using Cross-Join Pairs / E. Dubrova // Royal Institute of Technology (KTH). — 2011. — P. 13. — Режим доступа: <http://eprint.iacr.org/2011/632.pdf>
- [7] Distinguishing Attack on Grain / Shahram Khazaei, Mehdi Hassanzadeh, Mohammad Kiaei / Raymond Information and Communication Cryptographers. — 2005. — p. 9. Режим доступа: <http://cr.yp.to/streamciphers/grain/071.pdf>

Поступила в редколлегию 11.07.2014



Тимохін Сергій Сергійович, студент факультету комп'ютерних наук національного університету імені В. Н. Каразіна. Наукові інтереси: криптографія, криптоаналіз, симетричне та асиметричне шифрування.

Горбенко Іван Дмитрович, фото та відомості про автора див. на стор. 216.

УДК 004.056.55

Исследование и сравнительный анализ перспективных потоковых шифров / С.С. Тимохин, И.Д. Горбенко // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 217–220.

Потоковые симметричные шифры играют важную роль для защиты информации, для которой предъявляются значительные требования к уровню стойкости и скорости обработки в режиме он-лайн. Аппаратно-ориентированные потоковые шифры должны обеспечивать достаточный уровень устойчивости, быстродействия и быть компактными при аппаратной реализации. Нелинейные регистры сдвига является одним из подходов построения аппаратных шифров, что есть на сегодня мало исследованным и требует внимания.

Ключевые слова: потоковое шифрование, нелинейные регистры сдвига.

Табл.: 3. Ил.: 1. Библиогр.: 7 назв.

UDC 004.056.55

Research and comparative analysis of perspective stream ciphers / S.S. Timohin, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 217–220.

Streaming symmetric ciphers play an important role in information security for which significant demands to the level of resistance and processing speed in the on-line mode are made. Hardware-oriented stream ciphers should provide a sufficient level of security, speed of response and be compact in hardware implementation. Non-linear shift registers are one of the approaches to building hardware codes, which is currently slightly researched and requires attention.

Keywords: streaming encryption, nonlinear shift registers.

Tab.: 3. Fig.: 1. Ref.: 7 items.

НОВЫЙ ВЗГЛЯД НА ШИФР МУХОМОР

В.И ДОЛГОВ, И.В. ЛИСИЦКАЯ, К.Е ЛИСИЦКИЙ

Выполняется уточнение динамических показателей прихода шифра Мухомор к состоянию случайной подстановки. Показывается, что шифр Мухомор приходит к состоянию случайной подстановки уже на первом цикле, чего не позволяют все современные шифры. Делается вывод, что шифр Мухомор является на сегодняшний день самым прогрессивным решением по построению блочных симметричных шифров.

Ключевые слова: динамические показатели шифра, случайная подстановка, цикловое преобразование.

ВВЕДЕНИЕ

Мы здесь снова хотим возвратиться к обсуждению конструкторских решений, использованных при построении шифра Мухомор [1], представленного в своё время на украинский конкурс. В свете дальнейшего развития теории и практики построения современных шифров, последних работ по изучению динамических свойств шифров и анализа их цикловых преобразований [2, 3 и др.], появились новые результаты и взгляды, которые позволяют по иному взглянуть на показатели стойкости уже принятых решений, уточнить ранее выполненные оценки и показатели. Это в полной мере относится и к серии шифров Мухомор, хотя и ранее выполненные оценки [1, 4] уже выдвинули его в число лидеров современных методов построения блочных симметричных шифров.

В этой работе мы ещё раз обращаемся к решениям, принятым при построении шифров Мухомор, т. к. сегодня уже стало очевидным, что оценки, выполненные в предыдущих работах [2,3,5], существенно занижены и не раскрывают полностью перспективность использованных при построении этих шифров решений.

1. ДИНАМИЧЕСКИЕ ПОКАЗАТЕЛИ ПРИХОДА ШИФРОВ МУХОМОР К СОСТОЯНИЮ СЛУЧАЙНОЙ ПОДСТАНОВКИ

Дело в том, что при дополнительном анализе преобразований М-64, М-128 и М-256, удалось выявить повышенный запас стойкости шифров серии «Мухомор», который заключался в том, что конструкции цикловых функций этих шифров обеспечивают активизацию большего числа S-блоков, чем мы считали ранее.

Напомним здесь конструкцию цикловой функции М-128. Она представлена на рис. 1.

В соответствии с описанием шифра [1], входные 64-битовые значения функции М-128 меняются местами, затем полученный вектор делится на 4 части по 32 бита каждая. Эти значения складываются по модулю 2^{32} с соответствующей частью очередного подключа, поданного на вход функции. Затем каждое полученное 32-битовое слово проходит через SL преобразование, причём

результат преобразования складывается по модулю 2 со всеми остальными словами (см. рис. 1). Описанная операция выполнения SL преобразований над четырьмя 32-битовыми блоками выполняется 2 раза. Левое выходное 64-битовое слово формируется как результат конкатенации двух левых 32-битовых слов, правое 64-битовое слово – как результат конкатенации двух правых 32-битовых слов.

Сегодня мы считаем, что в представленных ранее результатах [2, 3] имеются, по крайней мере, две неточности.

1. Обратим здесь внимание на цепочку сложений по модулю 2 выхода самого правого SL преобразования первой и второй линейки SL преобразований цикловой функции со всеми выходами SL преобразований соответствующей линейки (см. рис. 1). Мы пришли к выводу, что эта цепь сложений по модулю два создаёт дополнительные активные S-блоки в каждой из колонок 32-битных слов (SL преобразований), число которых равно количеству активизированных S-блоков последнего в первой и второй линейках SL преобразования.

Мы это свойство сформулировали в виде утверждения:

Утверждение. При сложении по модулю два разностей выходов двух S-блоков результирующая вероятность прохода разностей для двух S-блоков равна произведению вероятностей прохода разностей для каждого из них.

В соответствии с этим положением динамические показатели прихода цикловой функции к случайной подстановки должны быть улучшены.

Этот момент мы уже учли в нашей работе [5].

Для иллюстрации развиваемого положения мы приведём здесь выдержку из этой работы.

«Функции усложнения М-128 шифра Мухомор-256 (вход в шифр 256 битов) состоит из восьми SL преобразований. Даже если считать, что на первом цикле задействованными являются минимум 29 S-блоков (точнее 33), формирующими все выходные байты цикла активными, то функция усложнения будет выходить к показателям случайной подстановки для 128-битного входа за один цикл и с показателями δ -равномерности равным 8-ми, 10-ти, 12-ти

и 16-ти (при $\delta = 16$ минимально необходимое число S-блоков есть 30). Эту функцию усложнения также можно применить для построения итеративного 128-битного шифра без надстройки Лея-Месси. Такой шифр будет обладать предельными динамическими характеристиками ($r_{\min} = 1$)».

Для самого же шифра Мухомор-256 уравнение зашифрования имеет вид $((2^{-5})^k = 2^{-248})$ и, следовательно, $k_{\min} = 49,6$. Для этого шифра $r_{\min} = 2$.

Действительно в представленном здесь результате считается, что первая линейка SL преобразований цикловой функции даёт один активный S-блок (входная разность в цикловую функцию первого цикла – это разность на входе одного из S-блоков последнего SL преобразования первой линейки). Во второй линейке возможен ещё один активный S-блок (МДР преобразование с вероятностью 2^{-59} даёт на выходе один активный байт), остальные МДР преобразования практически все будут да-

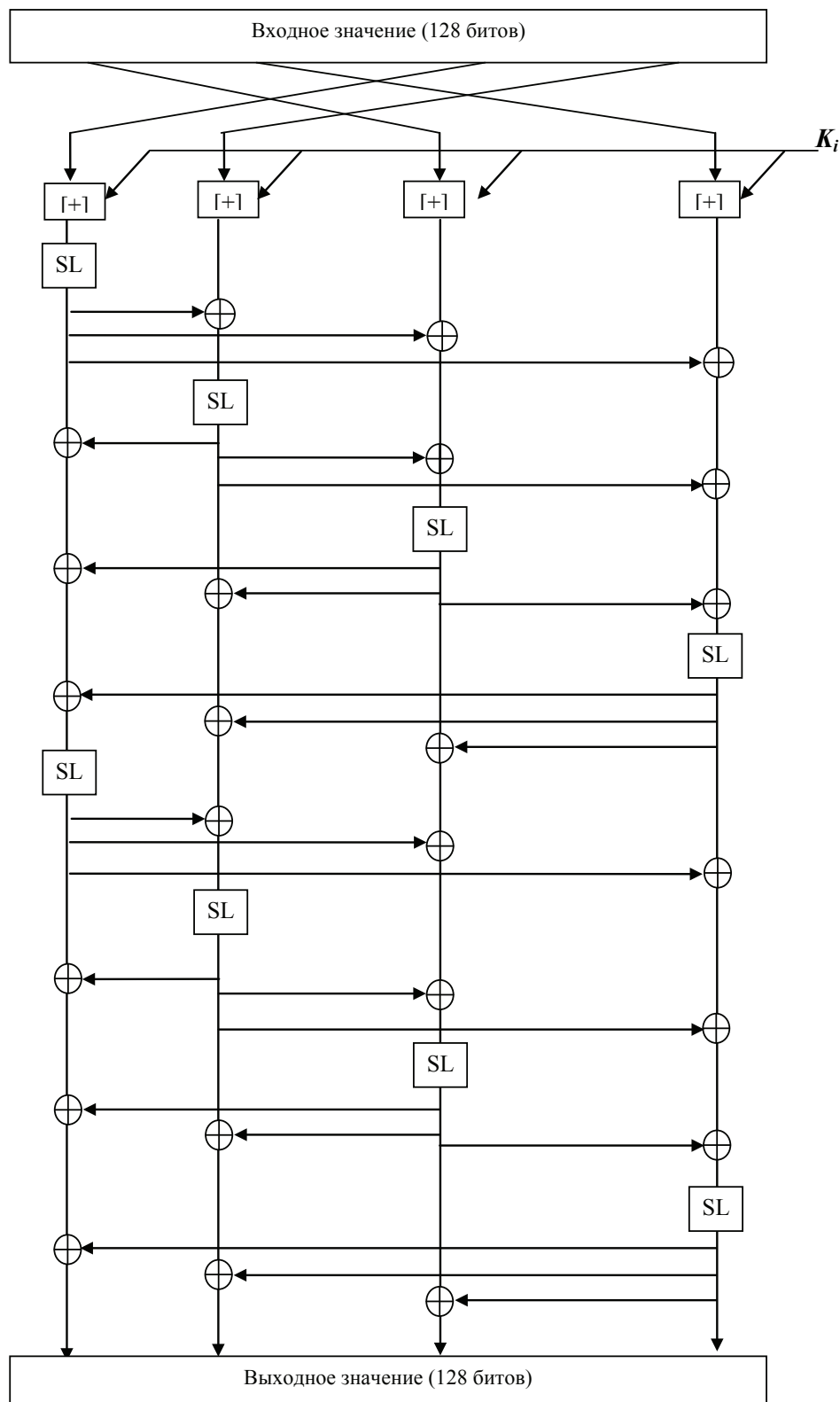


Рис. 1. Функция усложнения М-128

вать четыре активных S-блока. Тогда общее число активных S-блоков циклового преобразования получается на самом деле равным (близким к) $1 \times 4 + 1 + 7 \times 4 = 33$ вместо 29 (в предыдущем результате не учитываются суммирования на входах второй линейки SL преобразований с одноблочным выходом последнего SL преобразования первой линейки). Это действительно означает, что функция усложнения М-128 приходит к случайной подстановке за один цикл! (и по дифференциальным и по линейным показателям).

Но это ещё не всё!

2. Нам представляется, что надстройка шифра Мухомор в виде схемы Лея-Мэсси играет более важную роль в его конструкции, чем мы полагали ранее. Главная её цель, теперь мы считаем, это удвоить число активных S-блоков циклового преобразования шифра (длина блока данных при входе в цикловую функцию после прохода схемы усложнения удваивается). И тогда нужно считать, что в рассмотренном примере минимальное число активизированных S-блоков циклового преобразования шифра Мухомор-256, если исходить из ранее полученных 33-х активных S-блоков функции усложнения, получается равным 66-ти. Это значит, что сам шифр Мухомор-256 с родными S-блоками приходит к случайной подстановке уже на первом цикле. Адекватные выводы можно сделать и по отношению к другим конструкциям шифров серии Мухомор. Приведём далее расчёт динамических свойств шифра, построенного с использованием в качестве циклового преобразования функции усложнения М-256.

2. ПОКАЗАТЕЛИ СЛУЧАЙНОСТИ ШИФРА, ИСПОЛЬЗУЮЩЕГО В КАЧЕСТВЕ ЦИКЛОВОЙ ФУНКЦИИ ПРЕОБРАЗОВАНИЕ М-256

Выше уже было отмечено, что функции усложнения сами (без надстройки Лея-Мэсси) могут быть использованы для построения шифров. В этом параграфе мы приведём результаты оценки ожидаемых параметров перехода шифра, использующего в качестве цикловой функции преобразование М-256, к состоянию случайной подстановки.

В соответствии с идеей развиваемого в [2] подхода необходимо выполнить оценку минимального числа активных (задействованных S-блоков), после прохождения которых шифр становится случайной подстановкой. Это минимальное число определяется дифференциальными и линейными показателями самих S-блоков, применяемых в шифре, конструкциями и свойствами его цикловых преобразований, а также значениями показателей доказуемой стойкости шифра, зависящими от размера его битового входа. В работе [2] эта связь между отмеченными показателями определена в виде двух соотношений:

$$IPS_D = (DP_{\max}^{\pi})^k, \quad IPS_L = 2^{k-1} \cdot (LP_{\max}^{\pi})^k.$$

Здесь $DP_{\max}^{\pi}$ и $LP_{\max}^{\pi}$ — максимальные значения дифференциальной и линейной вероятностей подстановочных преобразований $\pi(x)$. IPS_D (Differential Indicator of Provable Security) — дифференциальный показатель доказуемой безопасности и IPS_L (Linear Indicator of Provable Security) — линейный показатель доказуемой безопасности, $k = k_{\min}$ — минимальное число активных S-блоков, участвующих в формировании перехода шифра к случайной подстановке.

Пользуясь расчётными соотношениями, установленными в работе [8], можно прийти к выводу, что ожидаемое значение максимума дифференциального перехода для шифра с 256-битным входом оказывается близким к 190, а ожидаемое значение максимума смещения линейного корпуса для шифра с 256-битным входом оказывается близким к 2^{130} . Соответственно получим, что максимальные значения линейной и дифференциальной вероятности для шифра с 256-битным входом получаются близкими друг к другу и равными приблизительно $2^{-248} \div 2^{-250}$ (близкими к сложности атаки полного перебора ключей).

Исходя из приведенных выше соотношений можно сделать вывод, что для шифра с 256-битным входом потребуется для прихода к состоянию случайной подстановки по дифференциальным переходам при использовании S-блоков с предельными показателями δ -равномерности равными $DP_{\max}^{\pi} = 2^{-6}$, (в соответствии с равенством $2^{-248} \approx (2^{-6})^k$) $k_{\min} = 41$ S-блок (для "родных" S-блоков с показателем δ -равномерности равными $DP_{\max}^{\pi} = 2^{-5}$ имеем $k_{\min} = 50$).

Аналогично, для прихода к состоянию случайной подстановки по линейным показателям при использовании S-блоков с предельными показателями нелинейности равными $LP_{\max}^{\pi} = 2^{-6}$ потребуется $(2^{-250} = 2^{k-1} \cdot (2^{-6})^k)$ $k_{\min} = 50$ S-блоков (для "родных" S-блоков с показателем нелинейности $LP_{\max}^{\pi} = 2^{-5}$ имеем $k_{\min} = 62,5$).

Расчёты числа активных S-блоков для этого случая приводят к результату: $1 \times 8 + 1 + 13 \times 4 = 61$. Для прихода к случайной подстановке за один цикл в шифре должны использоваться S-блоки с предельными показателями нелинейности.

3. СЛУЧАЙНЫЕ S-БЛОКИ В ШИФРЕ МУХОМОР

Оценим перспективы использования в шифре Мухомор случайных S-блоков. Будем здесь ориентироваться на функцию усложнения М-256.

Методика выполнения расчётов представлена в работе [3]. В табл. 1 представлены результаты расчётов числа переходов разного типа в 48-ми строках дифференциальной таблицы случайной подстановки. Мы в своих расчётах мето-

Таблица 1

Расчёт числа переходов разного типа в 48-ми строках дифференциальной таблицы случайной подстановки

Значение перехода таблицы	Число переходов дифференциальной таблицы	Число переходов в строке	Число переходов в 48 строках
12	1	0,003906	0,19
10	10	0,039065	1,87
8	104	0,40625	19,5
6	830	3,24218	155,62

дом перебора выбрали сразу такое число активных S-блоков, которое позволяет реализовать приход шифра к случайной подстановке. Для дифференциальных показателей оно равно 48.

Из представленных результатов следует, что для 48 активных S-блоков при выборе в строках максимально вероятных переходов можно ожидать при случайных входах в S-блоки:

- два перехода со значением 10;
- двадцать переходов со значением 8;
- двадцать пять переходов со значением 6.

Всего 48 переходов (48 активных S-блоков).

Вычисления в этом случае приводят к нужному результату:

$$\left(\frac{10}{256}\right)^2 \times \left(\frac{8}{256}\right)^{20} \times \left(\frac{6}{256}\right)^{26} = 2^{-250}.$$

Это означает, что использование случайных S-блоков также позволяет прийти шифру к состоянию случайной подстановки за два цикла.

Приведём теперь распределение переходов для смещений линейной аппроксимационной таблицы. В общее число переходов здесь входят и положительные и отрицательные смещения. Пользуясь результатами работы [6], можем рассчитать числа переходов разного типа в 70 строках линейной аппроксимационной таблицы случайной подстановки, итоги расчётов которых представлены в табл. 2.

Опять будем считать, что за счёт введения цикловых подключей входы в S-блоки будут случайными и статистически не зависимыми. Методика расчётов представлена в работе [3]. В таблице представлены результаты оценки числа переходов и их значений в 70 случайно взятых строках таблицы ЛАТ. Из результатов следует, что для 70 активных S-блоков при использовании максимально вероятных переходов можно ожидать при случайных входах в случайные S-блоки:

один переход со значением 32; три перехода со значением 30; восемь переходов со значением 28; восемнадцать переходов со значением 26; тридцать девять переходов со значением 24. Самый первый (один) S-блок взят с максимально возможным значением перехода (34).

Полагая далее, что строки в S-блок выбираются из всего множества 256-ти строк, при этом переходы по S-блокам идут в произвольном порядке и осуществляются по наиболее вероятному пути, можем выполнить оценку вероятности прихода шифра к состоянию случайной подстановки со случайными S-блоками. Вычисления для значения $k = 70$ приводят к результату

$$2^{69} \times \left(\frac{34}{128}\right)^2 \times \left(\frac{32}{128}\right)^2 \times \left(\left(\frac{30}{128}\right)^2\right)^3 \times \left(\left(\frac{28}{128}\right)^2\right)^8 \times \left(\left(\frac{26}{128}\right)^2\right)^{18} \times \left(\left(\frac{24}{128}\right)^2\right)^{39} = 2^{-257}$$

и, следовательно, 70 активных S-блоков позволяют осуществить переход шифра Мухомор-512 ($k_{\min} = 122$) к случайной подстановке за один цикл.

Напомним в заключение, что шифр Rijndael приходит к состоянию случайной подстановки по дифференциальным показателям на третьем цикле, а по линейным показателям лишь на четвёртом цикле.

Представленные результаты свидетельствуют о том, что шифры серии Мухомор не критичны к выбору S-блоков. Они обеспечивают предельные показатели стойкости и с S-блоками, выбранными случайным образом.

Более того, в качестве шифров с предельными криптографическими показателями могут выступать и шифры, использующие для построения своих цикловых преобразований функции усложнения М-64, М-128 и М-256.

Таблица 2

Расчёт числа переходов разного типа в 61-й строках линейной таблицы случайной подстановки

Значение перехода	Число переходов в таблице ЛАТ	Число переходов в строке таблицы ЛАТ	Число переходов в 70-ти случайно взятых строках таблицы ЛАТ
±34	1,998	0,0078	0,546
± 32	4	0,0156	1,092
± 30	10	0,0392	2,744
± 28	28	0,1098	7,686
± 26	65	0,2588	18,116
± 24	146	0,572	40,04
± 22	298	1,164	81,48

ВЫВОДЫ

По нашим оценкам шифр Мухомор является одним из самых прогрессивных решений по построению блочных симметричных шифров. Он обладает предельными на сегодняшний день показателями случайности — становится случайной подстановкой уже с первого цикла, чего не позволяет осуществить ни один из современных шифров. Представляется, что разработчики, не владея данными этой работы, перестраховались, определив число циклов для серии шифров Мухомор большее 10-ти (11, 13, 18). На самом деле в этом шифре без снижения показателей стойкости может использоваться существенно меньшее число циклов (вплоть до четырех), а это значит, что шифр может реализовать показатели быстродействия существенно превышающие соответствующие показатели многих известных шифров, в том числе и шифра Rijndael. На основании справедливости последнего утверждения мы остановимся в отдельной работе.

Литература

- [1] Горбенко И.Д. Перспективный блочный симметричный шифр «Мухомор» — основные положения та специфікація / И.Д. Горбенко, М.Ф. Бондаренко, В.И. Долгов, Р.В. Олійников та інші // Прикладная радиоэлектроника. — Харьков: ХТУРЭ. — 2007. — Том 6, №2. — С. 147–157.
- [2] Gorbenko I.D. On Ciphers Coming to a Stationary State of Random Substitution / I.D. Gorbenko, K.E. Lisitskiy, D.S. Denisov // Copyright © 2013 Horizon Research Publishing.
- [3] Горбенко И.Д. О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным / И.Д. Горбенко, К.Е. Лисицкий // Радиотехника: Всеукр. межвед. Науч.-техн. сб. — 2014. — Вып. № 176. — С. 27–39.
- [4] Бондаренко М.Ф. Обґрунтування вимог та розробка основних рішень з побудовання та властивості перспективного БСШ «Мухомор» / М.Ф. Бондаренко, И.Д. Горбенко, В.И. Долгов, Р. В. Олійников та ін. // Прикладная радиоэлектроника. — Харьков: ХНУРЭ. — 2007. — Том 6, № 2. — С. 174–185.
- [5] Лисицкий К.Е. Динамические показатели прихода блочных шифров к состоянию случайной подстановки [Текст] / К.Е. Лисицкий // Издательский дом LAP LAMBERT Academic Publishing, 2014. — 60 с.
- [6] Долгов Виктор Иванович. Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа: монография. / В.И. Долгов, И.В. Лисицкая. — Харьков. Издательство “Форт”, 2013. — 420 с.
- [7] Горбенко И.Д. Свойства и возможности оптимизации криптографических преобразований в AES — RIJNDAEL / И.Д. Горбенко, Д.А. Чекалин // Радиотехника. Всеукр. межвед.: науч.-техн. сб. 2001. Вып. 119. — С. 36–42.
- [8] Lisitskiy K.E. On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers [Text] / K.E. Lisitskiy // I.J. Computer Network and Information Security, 2014, 1, 11-18 Published Online November 2013 in MECS (<http://www.mecspress.org/>) DOI: 10.5815/ijcnis. 2014.01.02.

Поступила в редколлегию 21.07.2014

Долгов Виктор Иванович, фото и сведения об авторе см. на стр. 216.



Лисицкая Ирина Викторовна, доктор технических наук, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники. Область научных интересов: криптография, методы криптоанализа.

Лисицкий Константин Евгеньевич, фото и сведения об авторе см. на стр. 212.

УДК 621. 3.06

Новий погляд на шифр Мухомор / В. І. Долгов, І. В. Лисицька, К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 221–225.

Виконується уточнення динамічних показників приходу шифру Мухомор до стану випадкової підстановки. Показано, що шифр Мухомор приходить до стану випадкової підстановки вже на першому циклі, чого не дозволяють всі сучасні шифри. Робиться висновок, що шифр Мухомор є на сьогоднішній день найпрогресивнішим рішенням з побудови блокових симетричних шифрів.

Ключові слова: динамічні показники шифру, випадкова підстановка, циклове перетворення.

Табл.: 2. Іл.: 1. Бібліогр.: 8 найм.

UDC

A new view on the Muhomor cipher / V.I. Dolgov, I.V. Lisitskaya, K.E. Lisitsky // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 221–225.

A revision of dynamic indicators of the Muhomor cipher coming to the state of random substitution is performed. It is shown that the Muhomor cipher comes to the state of random substitution already at the first cycle, which all modern ciphers cannot do. It is concluded that the Muhomor code is by far the most advanced solution to build a symmetric block ciphers.

Keywords: dynamic cipher indicators, random substitution, round transformation.

Tab.: 2.: Fig.: 1. Ref.: 8 items.

АНАЛІЗ КОЛІЗІЙНИХ ВЛАСТИВОСТЕЙ РЕЖИМУ ВИРОБЛЕННЯ ІМІТОВСТАВОК ІЗ ВИБІРКОВИМ ГАМУВАННЯМ

О.О. КУЗНЕЦОВ, Д.В. ІВАНЕНКО, Є.П. КОЛОВАНОВА

Досліджується режим вироблення імітовставки із вибіркоким гамуванням, який призначено для забезпечення цілісності та конфіденційності повідомлень. Розглядаються основні криптографічні перетворення, які застосовуються в ході реалізації цього режиму, даються теоретичні оцінки ймовірності збігів (колізій) формованих імітовставок. Обґрунтовуються пропозиції щодо вдосконалення дослідженого режиму під час застосування в інформаційно-комунікаційних системах.

Ключові слова: колізія, гешування, імітовставка, криптографічний захист, блокове симетричне шифрування, цикл, підстановка.

ВСТУП

Однією з важливих складових забезпечення інформаційної безпеки є криптографічний захист інформації, тому дослідження сучасних криптоперетворень та обґрунтування перспективних напрямків зі створення надійних національних технологій захисту інформації є важливим та складним науковим завданням.

З метою побудови сучасних механізмів криптографічного захисту інформації широко застосовується блокове симетричне шифрування, яке полягає у перетворенні інформації з використанням ключових даних з метою приховування (відновлення) змісту інформаційного повідомлення, підтвердження його справжності, цілісності, авторства тощо. При цьому рівень захищеності інформації залежить не лише від властивостей блокового симетричного шифру, але і від режиму шифрування, під яким зазвичай розуміють такий метод його використання, який дозволяє реалізувати перетворення послідовності блоків відкритих даних у послідовність блоків зашифрованих даних із отриманням певних, наперед визначених криптографічних властивостей [10].

Надійним механізмом забезпечення цілісності та конфіденційності інформації в сучасних інформаційно-комунікаційних системах є режим формування імітовставки із вибіркоким гамуванням (Galois/Counter Mode and GMAC), специфікацію якого наведено у міжнародному стандарті NIST SP 800-38D [4]. Цей режим призначено для реалізації швидкого криптоперетворення при забезпеченні послуг безпеки інформації із використанням різних криптографічних примітивів, зокрема поліноміального гешування, гамування тощо.

Метою даної роботи є аналіз колізійних властивостей формованих імітовставок нового режиму шифрування Galois/Counter Mode and GMAC (GCM & GMAC) та обґрунтування умов його застосування в сучасних інформаційно-комунікаційних системах.

1. АНАЛІЗ КРИПТОПЕРЕТВОРЕНЬ GCM & GMAC

Новий режим шифрування Galois/Counter Mode and GMAC призначено для забезпечення послуг конфіденційності та цілісності даних,

перш за все, в ході реалізації інформаційно-комунікаційних протоколів, зокрема в межах протоколів безпеки IPSec.

Структурна схема режиму вироблення імітовставки із вибіркоким гамуванням GCM-AE_K (IV, P, A) наведено на рис. 1, де позначення 0^s визначає рядок довжини s, який складається з бітів '0'; len(X) — бітова довжина рядка X; [x]_s повертає бінарне представлення x як рядка бітової довжини s; MSBs(X) повертає s найбільш значущих бітів X; CIPH — затверджений 128-бітний блоковий симетричний шифр. Для забезпечення конфіденційності відкритого тексту P застосовується функція GCTR_K — деяка варіація режиму гамування [1–3], де перший блок лічильника для шифрування відкритого тексту генерується шляхом збільшення (inc₃₂) блоку J₀, сформованого з вектора ініціалізації IV. Для забезпечення цілісності застосовується інший механізм, який засновано на функції гешування GHASH_H. Функцію гешування використовують для стискання зашифрованих доданих автентифікованих даних A (Additional Authenticated Data — AAD) та шифротексту C в єдиний блок, який далі проходить шифрування для створення коду справжності T (імітовставки).

Зворотне перетворення полягає в перевірці справжності шифртексту C із доданими даними A та реалізується функцією GCM-AD_K (IV, C, A, T), структурну схему якої наведеною на рис. 2. При підтвердженні справжності (знов обчислений код T' дорівнює отриманому T) виконується розшифрування шифртексту C та формується відкритий текст P.

Таким чином, як видно з рис. 1 та 2, основними перетвореннями нового режиму Galois/Counter Mode and GMAC є гешування даних із використанням функції GHASH_H та шифрування/розшифрування функцією GCTR_K. Розглянемо їх більш детально.

На рис. 3 зображено структурну схему функції GCTR_K для реалізації шифрування/розшифрування, де ICB — початковий блок лічильника; CB_i — i-й блок лічильника; inc — функція лічильника. Шифрування відбувається за допомогою затвердженого блокового симетричного шифру AES зі 128-бітним розміром блоку з використанням ключа шифрування K.

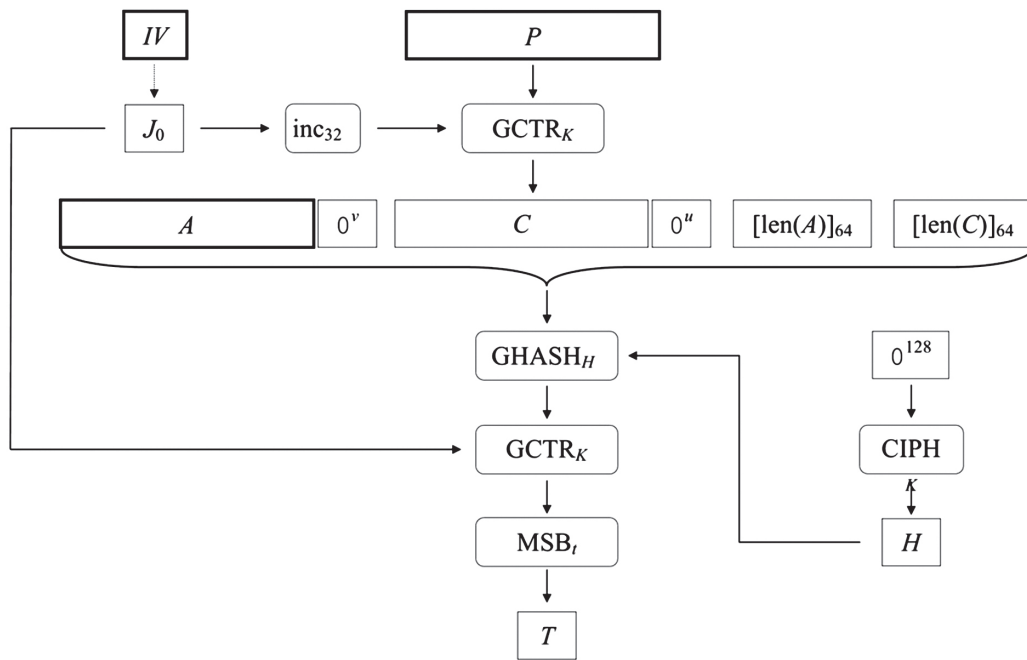


Рис. 1. $GCM - AE_K(IV, P, A) = (C, T)$

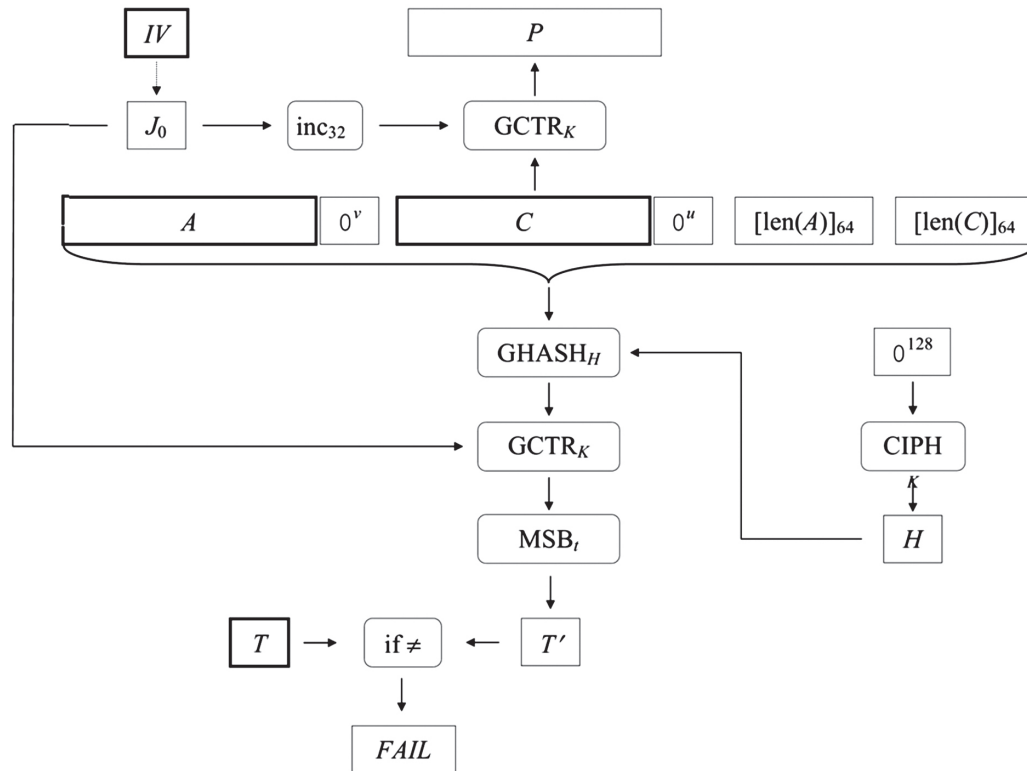


Рис. 2. $GCM - AD_k(IV, C, A, T) = \text{Paбо } FAIL$

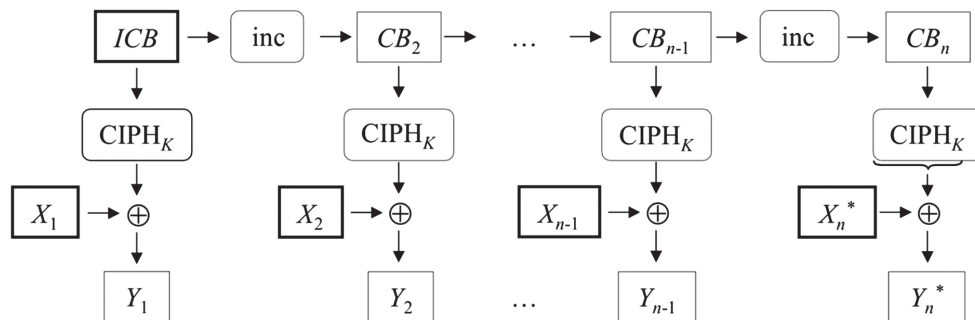


Рис. 3. $GCTR_K(ICB, X_1 \| X_2 \| \dots \| X_n^*) = Y_1 \| Y_2 \| \dots \| Y_n^*$

Для забезпечення цілісності інформації використовується функція гешування GHASH (див. рис. 1, 2). Цю функцію побудовано на основі поліноміальної схеми та реалізовано за допомогою множення на фіксований параметр – субключ з операціями в двійковому полі Галуа. На вхід функції подається деяка унікальна послідовність блоків довжиною m . Функція гешування GHASH розраховує геш-значення з використанням схеми Горнера, структуру якої зображено на рис. 4.

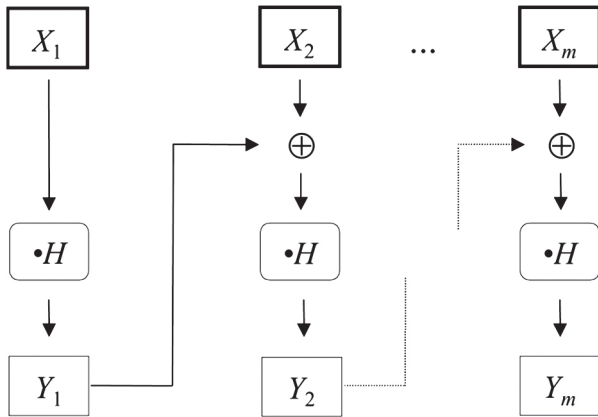


Рис. 4. $GHASH_H(X_1 \parallel X_2 \parallel \dots \parallel X_m) = Y_m$

Таким чином, проведений аналіз показав, що режим GCM & GMAC, який визначений у NIST Special Publication 800-38D: Galois/Counter Mode (GCM) and GMAC, містить такі криптоперетворення:

- шифрування/розшифрування відкритого тексту P функцією $GCTR_K$, яка по суті є деякою варіацією режиму гамування CTR [3, 4];
- обчислення геш-значення із використанням поліноміальної функції $GHASH_H$, яку використовують для стиснення шифротексту та автентифікованих даних A в єдиний блок;
- шифрування/розшифрування отриманого геш-значення, при цьому знову застосовується функція $GCTR_K$.

Отримане зашифроване геш-значення i є тим кодом справжності T , який призначено для забезпечення цілісності та автентичності інформації. За вітчизняною термінологією код T є імітовставкою, формування якої призначено для забезпечення захищеності від підміни та/або перекручування даних, здатності протистояти нав'язуванню помилкових повідомлень чи підміні повідомлення з метою зміни його сенсу.

Основним ймовірнісним показником ефективності режиму вироблення імітовставки (коду справжності, геш-значення) є ймовірність збігу (колізії) формованих кодів, тобто ймовірність такої події, коли для різних вхідних даних формовані імітовставки співпадають. Тобто ймовірність колізій визначає властивості формованих імітовставок щодо їх співпадіння на повній множині ключів та вхідних даних i є вихідним параметром щодо оцінки імітостійкості [10].

Проведемо дослідження колізійних властивостей розглянутої схеми вироблення імітовставок. Під час проведення досліджень зосередимо увагу на вивченні властивостей геш-кодів, що сформовано функцією поліноміального гешування $GHASH_H$, та вихідних кодів справжності (імітовставок), що сформовано за результатом роботи режиму GCM & GMAC загалом.

2. ДОСЛІДЖЕННЯ КОЛІЗІЙНИХ ВЛАСТИВОСТЕЙ ПОЛІНОМІАЛЬНОГО ГЕШУВАННЯ $GHASH_H$

Проведений аналіз показав, що при формуванні імітовставок у режимі GCM & GMAC використана функція гешування за поліноміальною схемою Горнера (функція $GHASH_H$). За визначенням вона належить до класу універсальних геш-функцій [5].

Ідеєю універсального гешування є визначення набору геш-функцій таким чином, що випадковий вибір функції забезпечить низьку ймовірність того, що будь-які два різних вхідних повідомлення X_a та X_b дадуть колізію, коли їх геш-значення розраховані з використанням функції із визначеної множини. Ймовірність виникнення такої колізії можна підрахувати так [5, 6]:

$$P_k = \delta_y(X_a, X_b) / |H|,$$

де P_k – ймовірність виникнення колізії, $\delta_y(X_a, X_b)$ – кількість співпадінь геш-значень, $|H|$ – потужність множини геш-функцій (або потужність множини ключів гешування, бо кожний ключ визначає окрему функцію із визначеної множини).

Для деякої геш-функції y та вхідних повідомлень X_a, X_b буде $\delta_y(X_a, X_b) = 1$ якщо $y(X_a) = y(X_b)$, та $\delta_y(X_a, X_b) = 0$ в іншому випадку. Тобто $\delta_y(X_a, X_b) = 1$ лише тоді, коли геш-значення від вхідних повідомлень X_a та X_b дадуть колізію. Для кінцевої множини H визначимо

$$\delta_H(X_a, X_b) = \sum_{y \in H} \delta_y(X_a, X_b).$$

Звідси $\delta_H(X_a, X_b)$ підраховує кількість геш-функцій (ключів гешування), які дають колізію для визначених X_a та X_b .

Згідно з [6] ймовірність виникнення колізії для функції гешування, яку побудовано на основі поліноміальної схеми, визначається як:

$$P_k = (n-1) / |H|, \quad (1)$$

де n – довжина вхідного повідомлення (кількість блоків вхідного повідомлення), $|H|$ – потужність множини ключів (потужність двійкового поля Галуа).

Дійсно, якщо правило гешування повідомлення $X = (X_1 \parallel X_2 \parallel \dots \parallel X_n)$ задається через обчислення у кінцевому полі $GF(2^k)$ значення поліному

$$Y_n = X_1 \cdot H_j^{n-1} \oplus X_2 \cdot H_j^{n-2} \oplus \dots \oplus X_n \cdot H_j^0, \quad (2)$$

де $H_j \in H$ – значення ключа гешування, $X_i, H_j \in GF(2^k)$, тоді колізія (співпадіння) геш-

значення Y_n із геш-кодом Y_n^* , який відповідає іншому повідомленню

$$X^* = (X_1^* \| X_2^* \| \dots \| X_n^*) \neq X = (X_1 \| X_2 \| \dots \| X_n)$$

відповідатиме випадку тотожності:

$$\begin{aligned} X_1 \cdot H_j^{n-1} \oplus X_2 \cdot H_j^{n-2} \oplus \dots \oplus X_n \cdot H_j^0 = \\ = X_1^* \cdot H_j^{n-1} \oplus X_2^* \cdot H_j^{n-2} \oplus \dots \oplus X_n^* \cdot H_j^0 \end{aligned}$$

для будь-якого введеного ключа гешування H_j .

Останнє рівняння перепишемо у канонічному вигляді:

$$\begin{aligned} (X_1 \oplus X_1^*) \cdot H_j^{n-1} \oplus (X_2 \oplus X_2^*) \cdot H_j^{n-2} \oplus \dots \\ \oplus (X_n \oplus X_n^*) \cdot H_j^0 = 0, \end{aligned} \quad (3)$$

отже колізія геш-значень, тобто подія $Y_n = Y_n^* |_{X \neq X^*}$ виникатиме лише тоді, коли H_j є коренем рівняння (3).

Однак за основною теоремою алгебри будь-який многочлен степеня $n-1$ має точно $n-1$ коренів з урахуванням їхньої кратності, тобто на безлічі значень $H_j \in H$ не більше $n-1$ різних ключів гешування обертаються в нуль ліву частину рівності (3). Таким чином, при рівноймовірному обранні ключів гешування $H_j \in H$ ймовірність колізії $P_k = P(Y_n = Y_n^* |_{X \neq X^*})$ визначатиметься за виразом (1).

Беручи до уваги зазначене вище, можна зробити висновок, що, обираючи підходяще значення потужності $|H|$ множини геш-функцій (ключів) та довжину вхідного повідомлення, можна досягти необхідного рівня ймовірності виникнення колізії. Графіки залежності ймовірності виникнення колізії від довжини повідомлення та потужності множини ключів для поліноміальної схеми наведено на рис. 5.

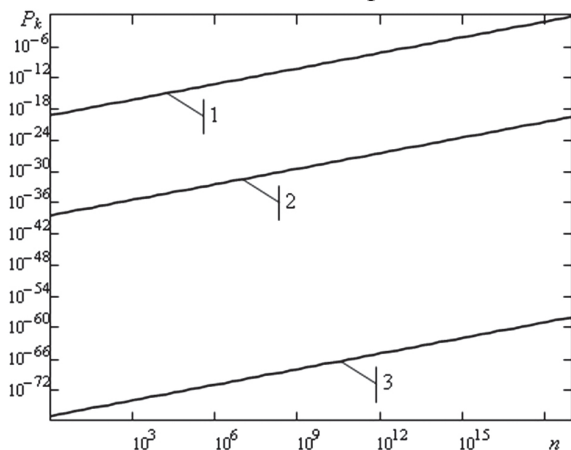


Рис. 5. Залежність ймовірності виникнення колізії від кількості блоків вхідного повідомлення:

1) $|H| = 2^{64}$; 2) $|H| = 2^{128}$; 3) $|H| = 2^{256}$

Як видно з наведених залежностей ймовірності колізій в ході застосування поліноміальної схеми гешування значно підвищується із збільшенням довжини вхідного повідомлення. При фіксованій довжині ключів гешування (та, відповідно, потужності $|H|$) ця залежність накладає додаткові обмеження на довжину пові-

домлень, які хешуються. Наприклад, для заданої ймовірності виникнення колізій $P_k = 2^{-32}$ та при довжині ключа гешування 128 бітів загальна кількість блоків повідомлення має задовольняти вимогу $n \leq 2^{96}$.

Обчислення геш-значення за правилом (2) має певні недоліки. Наприклад, якщо вхідне повідомлення складається лише з одного блоку, тоді формула (2) набуває вигляду $Y_1 = X_1 \cdot H_j^0 = X_1$ і правило гешування є тотожністю, тобто геш-значення дорівнюватиме блоку повідомлення і ключ гешування H_j при обчисленні Y_1 зовсім не використовується. Можливо саме тому в специфікації GCM & GMAC [4] застосовується дещо змінена поліноміальна форма обчислення геш-коду, а саме (див. рис. 4):

$$Y_m = X_1 \cdot H_j^m \oplus X_2 \cdot H_j^{m-1} \oplus \dots \oplus X_m \cdot H_j^1. \quad (4)$$

Випадок колізії спостерігатиметься так само під час виконання рівності:

$$\begin{aligned} X_1 \cdot H_j^m \oplus X_2 \cdot H_j^{m-1} \oplus \dots \oplus X_m \cdot H_j^1 = \\ = X_1^* \cdot H_j^m \oplus X_2^* \cdot H_j^{m-1} \oplus \dots \oplus X_m^* \cdot H_j^1, \end{aligned}$$

яку запишемо у вигляді

$$\begin{aligned} (X_1 \oplus X_1^*) \cdot H_j^m \oplus (X_2 \oplus X_2^*) \cdot H_j^{m-1} \oplus \dots \\ \oplus (X_m \oplus X_m^*) \cdot H_j^1 = 0, \end{aligned}$$

що після скорочення на H_j^1 повністю відповідає (3) із оцінкою ймовірності колізій (1).

Таким чином, правило обчислення геш-значень (4) є за колізійними властивостями тотожним правилу (2), але навіть у випадку гешування одного блоку обчислений геш-код $Y_1 = X_1 \cdot H_j$ залежить як від X_1 , так і від значення ключа гешування H_j .

Втім, слід відмітити недоліки застосованого правила (4). Якщо ключ гешування H_j дорівнює нулю, тоді геш-код також дорівнюватиме нулю для будь-якого вхідного повідомлення. Це накладає додаткові обмеження на схему формування ключових даних схеми гешування, втім специфікацією режиму GCM & GMAC ніяких обмежень та вказівок з цього приводу не наводиться [4]. Вказано лише, що субключ гешування H_j формується як зашифрована двійкова послідовність (див. рис. 1, 2).

Розглянемо цей випадок більш докладніше, бо формування нульового ключа гешування $H_j = 0$, як з'ясувалося, призводить до виродженої роботи поліноміальної схеми GHASH_H, і формована імітовставка T у цьому випадку зовсім не залежатиме від геш-коду повідомлення, а визначатиметься лише значенням вектора ініціалізації (синхроросилки) IV (див. рис. 1, 2).

Оцінимо ймовірність виникнення нульового субключа гешування, тобто ймовірність такої події, коли при шифруванні нульового вектора 0^{128} буде отримано значення $H_j = 0$. Для цього скористаємося деякими визначеннями та поняттями теорії підстановок [8].

3. ОЦІНКА ЙМОВІРНОСТІ ВИНИКНЕННЯ НУЛЬОВОГО СУБКЛЮЧА ГЕШУВАННЯ GHASH_n.

Розглянемо множину всіх бієктивних перетворень множини $Y = \{y_1, y_2, \dots, y_n\}$ саму в себе. Ці перетворення, які мають назву підстановок степеня n , утворюють групу відносно операції послідовного виконання перетворень. Така група має назву симетричної групи підстановок степеня n та позначається як S_n [8]. Її потужність визначається потужністю множини всіх підстановок степеня n , тобто дорівнює $n!$.

Кожній підстановці $s \in S_n$ відповідає єдина підстановка $s^{-1} \in S_n$, така, що

$$s^{-1} \cdot s(y) = s \cdot s^{-1}(y) = e(y), \quad y \in Y,$$

де $e(y) \in S_n$ — одинична підстановка, тобто $e(y) = y$ для всіх $y \in Y$.

Введемо такі позначення: $s \cdot s \cdot \dots \cdot s = s^k$, $s^{-1} \cdot s^{-1} \cdot \dots \cdot s^{-1} = s^{-k}$, де добутки містять k множників. Відповідно маємо $s^k \cdot s^{-k} = s^{-k} \cdot s^k = s^0 = e$.

Множина підстановок степеня n , яка є замкнутою відносно операції множення та обчислення оберненого для $s \in S_n$ елементу $s^{-1} \in S_n$, має назву групи підстановок. Кожна така група є підгрупою симетричної групи S_n [8].

Розглянемо деяку підстановку $s \in S_n$, яка діє на множині Y . Визначимо на множині Y бінарне відношення, при цьому вважатимемо $y \sim y'$ для $y, y' \in Y$, якщо існує таке j , що $y' = s^j(y)$. Це бінарне відношення є рефлексивним, симетричним та транзитивним, тобто є відношенням еквівалентності. Дійсно, відповідно до [8] маємо:

— $y \sim y$, оскільки $y = s^0(y) = e(y)$;

— із умови $y \sim y'$ випливає $y' \sim y$, оскільки із рівності $y' = s^j(y)$ випливає, що $y = s^{-j}(y')$;

— із $y \sim y'$ та $y' \sim y''$ випливає, що $y \sim y''$, бо з рівностей $y' = s^j(y)$ та $y'' = s^i(y')$ випливає, що $y'' = s^i(s^j(y)) = s^{i+j}(y)$.

Цикл s_i підстановки $s \in S_n$ довжини l_i визначається так:

$$s_i = (y, s_i^1(y), s_i^2(y), \dots, s_i^{l_i-1}(y)),$$

де $s_i^j(y) = y$.

Таким чином, довільну підстановку $s \in S_n$ можна розкласти на відповідні цикли [8]:

$$s = (y_1, s_1^1(y_1), s_1^2(y_1), \dots, s_1^{l_1-1}(y_1)) \dots (y_k, s_k^1(y_k), s_k^2(y_k), \dots, s_k^{l_k-1}(y_k)). \quad (5)$$

Наприклад, підстановка s степеня 4-го виду

$$s = \begin{pmatrix} y_1 & y_2 & y_3 & y_4 \\ s(y_1) & s(y_2) & s(y_3) & s(y_4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

може бути подана у вигляді розкладу на 3 цикли:

$$s_1 = (y_1) = (1), \quad l_1 = 1;$$

$$s_2 = (y_2, s_2^1(y_2)) = (2, 4), \quad l_2 = 2;$$

$$s_3 = (y_3) = (3), \quad l_3 = 1,$$

тобто маємо такий розклад:

$$s = (y_1)(y_2, s_2^1(y_2))(y_3) = (1)(2, 4)(3).$$

Загалом, підстановка $s \in S_n$ належить до циклового класу $\{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}\}$, якщо вона містить α_1 циклів довжини 1, α_2 циклів довжини 2, і т. д., тобто:

$$s = (y_1)(y_2) \dots (y_{\alpha_1})(y'_{\alpha_1}, y''_{\alpha_1})(y'_2, y''_2) \dots (y'_{\alpha_2}, y''_{\alpha_2}) \dots,$$

$$1\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n.$$

Позначимо через $C(\alpha_1, \alpha_2, \dots, \alpha_n)$ число підстановок у цикловому класі $\{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}\}$, а через $C(n, k)$ — число підстановок степеня n , які мають k циклів. Тоді маємо [8]:

$$C(\alpha_1, \alpha_2, \dots, \alpha_n) = \frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!},$$

$$C(n, k) = \sum_{\substack{1\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n \\ \alpha_1 + \alpha_2 + \dots + \alpha_n = k, \alpha_i \geq 0}} \frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!} = |s(n, k)|, \quad (6)$$

де $s(n, k)$ — числа Стірлінга першого роду, які визначаються через співвідношення:

$$x(x-1) \dots (x-n+1) = \sum_{k=0}^n s(n, k) x^k.$$

На множині всіх підстановок степеня n , які утворюють симетричну групу S_n , задамо рівномірний ймовірнісний розподіл, тобто кожній вибраній підстановці $s \in S_n$ поставимо у відповідність ймовірність її обрання, що дорівнює $1/n!$. За сучасними поглядами симетричної криптографії така множина рівномірних відображень відповідає уявленню про «ідеальний» шифр, бо якщо обрання окремої підстановки $s \in S_n$ пов'язати із значенням введенного ключа шифрування, тоді отримане перетворення відповідатиме випадковому і рівномірно вибраному шифру тексту для кожного відкритого тексту при будь-якому ключі, тобто на всіх можливих варіантах відображень відкритого тексту у шифрограму.

За визначенням блоковий симетричний шифр є функцією відображення множини текстів і множини ключів у множину шифртекстів: $E: K \times M \rightarrow E$, де K , M та E — множини ключів, відкритих та шифртекстів, відповідно. Для шифру AES потужність множини ключів $|K| \in \{2^{128}, 2^{192}, 2^{256}\}$, а $|M| = |E| = 2^{128}$. Оскільки при зашифруванні необхідно мати можливість відновити текст за допомогою ключа, потрібно, щоб для всіх ключів $k \in K$ функція зашифрування була перестановкою (підстановкою), тобто відображення $E: K \times M \rightarrow E$ має бути бієктивним.

На практиці для довільного n -бітового блокового шифру існує $2^n!$ можливих перестановок відкритого тексту. Практично це означає, що кількість бітів ключа, яку необхідно для отримання всіх можливих перестановок, становить близько $\ln 2^n! \approx n \cdot 2^n$ бітів¹. Утім розмір ключа більшості блокових шифрів не перевищує невеликого числа, кратного розміру блоку, відповідно такі шифри можуть забезпечити лише невелику частку від повної кількості можливих перестано-

¹ За формулою Стірлінга $\ln(x!) = x \ln(x) - x - O(\ln(x))$

вок. Наприклад, для 128-бітного шифру AES маємо $2^{128} \approx 2^{128 \cdot 2^{128}}$ можливих перестановок 128-бітових блоків, з яких, залежно від довжини ключа, використовується тільки 2^{128} , 2^{192} або 2^{256} перетворень. Таким чином, кожен шифр є деяка підмножина повної множини всіх можливих підстановок, що діють на множині блоків оброблюваних даних. Основне припущення, яке приймається при обґрунтуванні стійкості симетричного криптоперетворення полягає саме у збереженні ймовірнісних властивостей випадкової підстановки, тобто припускається, що хоча при шифруванні і застосовується обмежений набір підстановок із S_n , та певні розподіли ймовірностей елементів цієї підмножини відповідають властивостям випадково і рівномірно обраної підстановки із всієї множини S_n .

Проведемо дослідження цих розподілів з метою оцінки ймовірності виникнення нульового шифр-тексту при шифруванні нульового відкритого тексту. Для цього розглянемо випадкову величину ξ_n , яка дорівнює числу циклів у випадково вибраній підстановці $s \in S_n$. Оцінимо ймовірність випадкової події $\xi_n = k$, тобто такого випадку, коли у випадково вибраній підстановці спостерігатиметься точно k циклів (див. вираз (5)). З формули (6) безпосередньо впливає вираз для точного розподілу ймовірностей через числа Стірлінга першого роду:

$$P(\xi_n = k) = \frac{C(n, k)}{n!} = \frac{|s(n, k)|}{n!}, \quad k = 0, 1, \dots, n.$$

У роботах [8, 15] отримано математичне очікування $M\xi_n$ та дисперсію $D\xi_n$ випадкової величини ξ_n :

$$M\xi_n = \sum_{j=1}^n \frac{1}{j} = \ln n + C + o(1), \quad C = 0,5772\dots,$$

$$D\xi_n = \sum_{j=1}^n \frac{1}{j} - \sum_{j=1}^n \frac{1}{j^2} = \ln n + C + o(1),$$

крім того показано, що при $n \rightarrow \infty$ випадкова величина $\xi'_n = (\xi_n - \ln n) / (\ln n)$ розподілена асимптотично нормально з параметрами $(0, 1)$, тобто

$$\lim_{n \rightarrow \infty} P(\xi'_n < u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^u e^{-y^2/2} dy.$$

У роботах [11–14] досліджено емпіричний розподіл ймовірності виникнення циклу певної довжини у зменшених моделях шифру, встановлено, що цей розподіл дуже близький до розглянутого теоретичного розподілу випадкової підстановки, тобто за цим критерієм можна стверджувати, що шифр за розподілом кількості циклів подібний властивостям випадкової підстановки. Водночас для оцінки ймовірності виникнення нульового субключа гешування в схемі GCM & GMAC потрібна інша характеристика шифру, а саме розподіл числа циклів заданої довжини. Відповідно до [8], ця характеристика у випадковій підстановці визначається наступним чином.

Позначимо як $\chi_{n,l}$ число циклів довжини l у випадковій рівномірній підстановці степеня n . Тоді розподіл ймовірностей випадкової події $\chi_{n,l} = k$ визначається як:

$$P(\chi_{n,l} = k) = \frac{1}{l^k k!} \sum_{j=0}^{[n/l]-k} \frac{(-1)^j}{l^j j!}, \quad k = 0, 1, \dots, [n/l]. \quad (7)$$

При $n \rightarrow \infty$ випадкова величина $\chi_{n,l}$ має в межах розподіл Пуассона з параметрами $\lambda = 1/l$, тобто

$$\lim_{n \rightarrow \infty} P(\chi_{n,l} = k) = \frac{1}{l^k k!} e^{-1/l}, \quad k = 0, 1, \dots$$

Скористаємося формулою точного розподілу ймовірностей випадкової події $\chi_{n,l} = k$ у вигляді (7). Значення $n!P(\chi_{n,l} = k)$ відповідає кількості підстановок, які містять k циклів довжини l . Нас цікавить кількість підстановок, які обов'язково мають цикли довжини $l=1$, причому ці цикли мають переводити фіксований елемент y з множини Y сам у себе. Тобто необхідно оцінити кількість таких підстановок $s \in S_n$, які для визначеного $y \in Y$ містять цикли $s(y) = y$ довжини $l=1$. У криптографії при розгляді блокових симетричних криптоперетворень такі випадки прийнято називати фіксованими точками підстановки [11].

Для $l=1$ формула (7) набуде вигляду

$$P(\chi_{n,l=1} = k) = \frac{1}{k!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!}, \quad k = 0, 1, \dots, n,$$

причому для $k=1, \dots, n$ кожен з $n!P(\chi_{n,l=1} = k)$ випадків для фіксованого $y \in Y$ спостерігатиметься

$$\frac{C_{n-1}^{k-1}}{C_n^k} = \frac{(n-1)!}{(k-1)!(n-k)!} \frac{k!(n-k)!}{n!} = \frac{k}{n}$$

разів, тобто кількість фіксованих точок $s(y) = y$ для визначеного $y \in Y$ визначатиметься за формулою:

$$\sum_{k=1}^n n!P(\chi_{n,l=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = \sum_{k=1}^n \left(\frac{(n-1)!}{(k-1)!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!} \right) = (n-1)!,$$

а відповідна ймовірність фіксованої точки у випадковій рівномірній підстановці степеня n матиме вигляд:

$$\sum_{k=1}^n P(\chi_{n,l=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = \frac{(n-1)!}{n!} = \frac{1}{n}. \quad (8)$$

Останній вираз може бути отриманий значно простіше з тривіальних комбінаторних міркувань. Дійсно, якщо на множині $Y = \{y_1, y_2, \dots, y_n\}$ зафіксувати m елементів, тоді можливі $(n-m)!$ варіантів перестановок решти елементів. Тобто на всій множині підстановок з S_n при їх випадковому рівномірному розподілі ймовірність обрати підстановку з m фіксованими точками дорівнюватиме

$$\frac{(n-m)!}{n!} = \frac{1}{(n-m+1)(n-m+2)\dots n} = \frac{1}{(n)_m}, \quad (9)$$

що при $m=1$ співпадає з (8) ².

² $(n)_m = n(n-1)\dots(n-m+1)$ — загальноприйняте позначення спадаючого факторіалу

Припустимо, що n -бітний блоковий симетричний шифр, який складається з деякої підмножини симетричної групи підстановок степеня 2^n , відповідає ймовірнісним властивостям випадкової підстановки, зокрема припустення, що на всій множині ключів шифру, які задають обрання конкретної підстановки s із S_{2^n} , ймовірність обрати підстановку з m фіксованими точками визначатиметься за (9), тобто дорівнюватиме

$$\frac{(2^n - m)!}{2^n!} = \frac{1}{(2^n)_m}.$$

Тоді кількість ключів шифру, які призведуть до появи m фіксованих точок $s(y) = y$ для визначених блоків відкритого тексту $y \in Y$ визначатиметься за формулою $N(m) = \frac{2^k}{(2^n)_m}$, де k — бітова

довжина ключа шифру.

Зокрема, для випадку $m = 1$ маємо

$$N(m=1) = \frac{2^k}{(2^n)_1} = 2^{k-n},$$

тобто:

— якщо $k < n$ з високою ймовірністю можна стверджувати, що шифр не містить фіксованих точок, тобто на всій множині ключів шифрування не знайдеться жодного, який призведе до появи хоча б одного нешифрованого відкритого тексту;

— якщо $k = n$ з високою ймовірністю знайдеться один ключ із $|K| = 2^k$ можливих, який призведе до появи фіксованої точки, тобто отримаємо випадок нешифрованого відкритого тексту;

— якщо $k > n$ кількість ключів, які призводять до появи фіксованої точки, стрімко зростає, їх кількість експоненційно залежить від бітової довжини ключа.

У випадку застосування шифру AES маємо таке:

— при довжині ключа $k = 128$ бітів один ключ створюватиме фіксовану точку, тобто, наприклад, спостерігатиметься випадок, коли при шифруванні нульового вектору 0^{128} буде отримано значення $H_j = 0$;

— при довжині ключа $k = 192$ бітів загалом $2^{k-n} = 2^{64}$ ключів будуть створюватимуть фіксовану точку, тобто випадок із шифруванням нульового вектору 0^{128} в нульове значення $H_j = 0$ спостерігатиметься 2^{64} разів;

— при довжині ключа $k = 256$ бітів вже $2^{k-n} = 2^{128}$ ключів відповідатимуть випадку шифрування нульового вектору 0^{128} в те ж саме значення, тобто в $H_j = 0$.

Отримані оцінки дозволяють стверджувати, що в ході виконання зроблених припущень, ймовірність виникнення фіксованої точки шифру не залежить від довжини ключа, вона визначається лише довжиною блоків даних, які обробляє

шифр. Цей висновок збігається із загальною інтерпретацією шифру як випадкової підстановки, фіксовані точки в якій — звичайне явище. Однак для розглянутого вище ключового поліноміального гешування випадки фіксованих точок для нульового блоку є неприпустимими, бо це повністю спотворює схему формування геш-значень, які вже не залежатимуть від вихідних даних, колізійні властивості порушуються і не відповідають теоретичним оцінкам. Очевидно, що зі збільшенням потужності множини ключів кількість фіксованих точок також зростатиме і число так би мовити «слабких» ключів, які призводять до виродженої роботи функції гешування, збільшується пропорційно потужності ключового простору.

Розглянемо тепер вплив останнього шару перетворень режиму GCM & GMAC, зокрема шифрування/розшифрування, отриманого за допомогою функції GHASH_n геш-значення, оцінимо ймовірності показники формованих імітовставок.

4. ДОСЛІДЖЕННЯ КОЛІЗІЙНИХ ВЛАСТИВОСТЕЙ, ФОРМОВАНИХ РЕЖИМОМ GCM & GMAC ІМІТОВСТАВОК

Останній шар перетворень режиму GCM & GMAC полягає у застосуванні функції GCTR_k, яка по суті є деякою варіацією режиму гамування CTR [3, 4]. Тобто до отриманого на попередньому шарі перетворень геш-значення додається результат зашифрування деякого вектору J_0 , який отримано із вектора ініціалізації IV (див. рис. 1, 2). Тобто фактично, до сформованого геш-значення додається зашифрована константа, яка формується встановленим порядком.

Відповідно до специфікації режиму GCM & GMAC на формування вектора ініціалізації (за вітчизняною термінологією — синхропосилка) накладаються такі обмеження:

— ймовірність того, що при обчисленні імітовставок для двох різних вихідних даних будуть застосовані однакові вектори ініціалізації при однакових ключах, не має бути більшою, ніж 2^{-32} ;

— для кожного заданого ключа повне число формованих імітовставок для будь-яких вихідних повідомлень не має перевищувати 2^{32} .

Перша умова визначає максимальну ймовірність застосування однакових параметрів криптографічного перетворення для різних вихідних даних. Тобто навіть, якщо при введеному ключі та векторі ініціалізації виникне колізія (співпадіння імітовставок для різних вихідних даних), ця подія буде повторена не частіше ніж один раз на 2^{32} ³.

Друга умова визначає максимальну кількість можливих застосувань режиму GCM & GMAC для кожного з введених ключів, тобто ця умова задає обмеження на термін дії ключа. Разом

³ Це твердження не враховує випадку, коли колізія імітовставок відбувається при різних параметрах криптоперетворення

з першою умовою вона визначає, що кожен ключ буде поєднаний із деяким вектором ініціалізації тільки один раз, тобто в ході оброблення різних вихідних даних одні й ті ж пари «ключ — вектор ініціалізації» застосовуватися двічі не будуть ніколи.

Таким чином можна зробити такі висновки:

— для кожного введенного ключа в ході оброблення різних вихідних даних щоразу застосовуватимуться різні вектори ініціалізації;

— для кожного введенного вектора ініціалізації в ході оброблення різних вихідних даних щоразу застосовуватимуться різні ключі;

— одні й ті ж самі вихідні дані можуть бути оброблені із застосуванням одного і того ж самого вектора ініціалізації, але ключі щоразу мають бути різними;

— одні й ті ж самі вихідні дані можуть бути оброблені із застосуванням одного і того ж самого ключа, але вектори ініціалізації щоразу мають бути різними.

Тобто, якщо повторюється ключ — тоді не мають повторюватися вектори ініціалізації, а якщо повторюється вектор ініціалізації — мають бути різними ключі.

Позначимо через

$$Y_m = \text{GHASH}_H(X_1 \parallel X_2 \parallel \dots \parallel X_m)$$

результат поліноміального гешування як на рис. 4, а через $T = \text{MSB}_t(\text{GCTR}_K(J_0, Y_m)) = \text{MSB}_t(Z \oplus Y_m)$ формовану імітовставку як на рис. 1, 2, де $Z = \text{CHIP}_K(J_0)$ результат зашифрування J_0 на ключі K .

Очевидно, що колізійні властивості формованих імітовставок залежать як від властивостей геш-значень Y_m , так і від результатів зашифрування Z . Колізійні властивості Y_m було оцінено у розділі 3. Оцінимо ймовірність співпадиння Z та кінцевих результатів T .

За визначенням блоковий симетричний шифр є бієктивним відображенням, тому різні вихідні значення J_0 після зашифрування будуть співставленні із різними значеннями Z , тобто колізій не виникатиме. Із умов формування векторів ініціалізації, які розглянуто вище, випливає, що навіть для однакових вихідних повідомлень $(X_1 \parallel X_2 \parallel \dots \parallel X_m)$ і однакових ключів відповідні J_0 будуть різними, тобто ймовірність колізій проміжних значень Z завжди дорівнюватиме нулю.

Розглянемо тепер умови колізій імітовставок, зокрема такий випадок, коли для різних вихідних повідомлень $(X_1 \parallel X_2 \parallel \dots \parallel X_m)$ на однаковому ключі K відповідні результати $Z \oplus Y_m$ будуть тотожними. Така умова формально може бути подана у вигляді:

$$Z \oplus Y_m = Z' \oplus Y'_m, \quad (10)$$

де Z і Y_m є проміжними результатами формування імітовставки для вихідного повідомлення $(X_1 \parallel X_2 \parallel \dots \parallel X_m)$, а Z' і Y'_m є відповідними

значеннями для іншого повідомлення $(X'_1 \parallel X'_2 \parallel \dots \parallel X'_m) \neq (X_1 \parallel X_2 \parallel \dots \parallel X_m)$.

Вище показано, що для таких повідомлень завжди виконується нерівність $Z \neq Z'$ і умова (10) виконуватиметься лише при $Y_m \oplus Y'_m = Z \oplus Z' \neq 0^{128}$, тобто лише тоді, коли не виникатиме колізій геш-значень Y_m та Y'_m .

Останній висновок найбільш вражаючий, оскільки метою поліноміального гешування було саме зменшення ймовірності колізій формованих геш-значень. Точне значення ймовірності колізій формованих імітовставок визначатиметься комбінаторними властивостями шифру, тобто залежатиме від кількості випадків $Y_m \oplus Y'_m = Z \oplus Z'$. Однак можна з впевненістю стверджувати, що колізійні властивості імітовставок не повторюватимуть відповідні властивості геш-значень, що досліджувалися у розділі 3.

ВИСНОВКИ

Проведений аналіз показав, що для використання в режимі шифрування Galois/Counter Mode and GMAC визначеної функції поліноміального гешування GHASH_H мають бути застосовані певні обмеження, зокрема не можна використовувати нульовий субключ гешування, оскільки при цьому значення функції завжди обертається в нуль для будь-якого вхідного повідомлення, що створює передумови для зниження рівня імітостійкості. Це є неприпустимим, бо схема формування геш-значень спотворюється, формовані імітовставки не залежатимуть від вихідних даних, колізійні властивості порушуються і не відповідають теоретичним оцінкам.

В ході досліджень було з'ясовано, що випадок формування нульового субключа поліноміального гешування GHASH_H виникає за наявності фіксованих точок шифру, тобто таких ключів, які шифрують нульову послідовність саму у себе. Отримані оцінки показують, що ймовірність виникнення фіксованої точки шифру не залежить від довжини ключа, вона визначається лише довжиною блоків даних, які обробляє шифр. Зі збільшенням потужності множини ключів кількість фіксованих точок також зростає і число «слабких» ключів, які призводять до виродженої роботи функції гешування збільшується пропорційно потужності ключового простору. У випадку застосування шифру AES при довжині ключа $k = 128$ бітів один ключ створюватиме фіксовану точку; при довжині ключа $k = 192$ бітів загалом $2^{k-n} = 2^{64}$ ключів створюватимуть фіксовану точку; при довжині ключа $k = 256$ бітів $2^{k-n} = 2^{128}$ ключів відповідають випадку шифрування нульового вектора 0^{128} в те ж саме значення, тобто відповідають формуванню нульового субключа гешування.

Ймовірність колізій формованих імітовставок визначатиметься комбінаторними властивостями шифру, тобто залежатиме від кількості

випадків, коли бітова різниця зашифрованих на одному ключі різних констант дорівнюватиме бітовій різниці сформованих на цих же ключах геш-значень. Випадок колізій імітовставок можливий лише для різних геш-значень. Емпірична оцінка числа колізій та відповідні оцінки ймовірностей із застосуванням зменшених моделей шифрів є перспективним напрямком подальших досліджень. Перспективним також є перевірка зроблених припущень щодо тотожності деяких властивостей випадкової підстановки певним характеристикам застосовуваного шифру, зокрема це безпосередньо відноситься до вивчення ймовірнісних властивостей виникнення фіксованої точки та, що еквівалентно, кількості циклів довжини $l=1$.

Література

- [1] ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Изд-во стандартов, 1989. — 20 с.
- [2] ГОСТ Р ИСО/МЭК 10116-93. Информационная технология. Режимы работы для алгоритма n -разрядного блочного шифрования. [Электронный ресурс]. Режим доступа: <http://docload.spb.ru>
- [3] ISO/IEC 10116. Information technology — Security techniques — Modes of operation for an n -bit block cipher. [Электронный ресурс]. Режим доступа: <http://www.iso.org>
- [4] NIST Special Publication 800-38D. Block Cipher Modes. [Электронный ресурс]. Режим доступа: <http://csrc.nist.gov>
- [5] Stinson D.R. Universal hashing and authentication codes // Designs, Codes and Cryptography — 1994. — Volume 4, Issue 3. — pp. 369–380.
- [6] Polynomial hashing: 4,588,985 United States Patent: H 03 M 7/00, field of search 340/347 DD / Carter J. L., Wegman M. N.; International Business Machines Corporation, Armonk, N.Y. — filed Dec. 30, 1983 — May 13, 1986
- [7] Raphael Chung-Wei Phan. Mini Advanced Encryption Standard (Mini-AES): A testbed for Cryptanalysis Students // Cryptologia, XXVI(4), October 2002. P. 283–306.
- [8] Сачков В.Н. Введение в комбинаторные методы дискретной математики. — М.: Наука. Гл. ред. физ.-мат. лит., 1982. — 384 с.
- [9] Тронин С.Н. Введение в теорию групп. — Казань: Казанский государственный университет, 2006. — 100 с.
- [10] Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. — Харків: Вид-во «Форт», 2013. — 880 с.
- [11] Долгов В.И., Лисицкая И.В., Руженцев В.И. Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника — 2007. — Т. 6, № 2. — С. 257–263.
- [12] Кузнецов А.А., Лисицкая И.В., Исаев С.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс // Прикладная радиоэлектроника. — 2011. — Т. 10, № 2 — С. 135–140.
- [13] Сорока Л.С., Кузнецов А.А., Московченко И.В., Исаев С.А. Исследование дифференциальных свойств блочно-симметричных шифров. // Системы обработки информации. — X: ХУПС. — 2010 — Вип. 6(87). — С. 286–294.
- [14] Долгов В.И., Родинко М.Ю. Блочные симметричные шифры — случайные подстановки. Комбинаторные показатели // Прикладная радиоэлектроника — 2013. — Т.12, №2 — С. 236–239.
- [15] Александров П.С. Введение в теорию групп. — М.: Наука, — 1980. — 145 с.

Надійшла до редколегії 13.08.2014

Кузнецов Олександр Олександрович, фото та відомості про автора див. на стор. 207.

Іваненко Дмитро Вікторович, фото та відомості про автора див. на стор. 207.

Колованова Євгенія Павлівна, фото та відомості про автора див. на стор. 207.

УДК 004.056.55

Анализ коллизионных свойств режима выработки имитовставок с выборочным гаммированием / А. А. Кузнецов, Д. В. Иваненко, Е. П. Колованова // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 226–234.

Исследуется режим выработки имитовставки с выборочным гаммированием, который предназначен для обеспечения целостности и конфиденциальности сообщений. Рассматриваются основные криптографические преобразования, которые используются при реализации этого режима, приводятся теоретические оценки вероятности коллизий сформированных имитовставок. Обосновываются предложения по усовершенствованию исследуемого режима при использовании в информационно-коммуникационных системах.

Ключевые слова: коллизия, хеширование, имитовставка, криптографическая защита, блочное симметричное шифрование, цикл, подстановка.

Ил.: 5. Библиогр.: 15 назв.

UDK 004.056.55

Analysis of collision properties of the mode of generating message authentication codes with selective gamming / A.A. Kuznetsov, D.V. Ivanenko, E.P. Kolovanova // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 226–234.

The paper investigates the mode of generating a message authentication code with selective gamming which is designed to ensure the integrity and confidentiality of communications. Basic cryptographic transformations are considered that are used to implement this mode, theoretical estimates of collisions probability are provided. Offers to improve the mode under study are justified when used in information and communication systems.

Keywords: collision, hashing, authentication code, cryptographic protection, block symmetric encryption, cycle, substitution.

Fig.: 5. Ref.: 15 items.

ВЕРОЯТНОСТИ ДВУХЦИКЛОВЫХ ДИФФЕРЕНЦИАЛОВ RIJNDAEL-ПОДОБНОГО ШИФРА С ПРОИЗВОЛЬНЫМИ ПОДСТАНОВКАМИ

В.И. РУЖЕНЦЕВ

Работа посвящена анализу двухцикловых дифференциалов Rijndael-подобного шифра. Предложенный в одной из предыдущих работ подход к оценке вероятностей дифференциалов применяется для шифров с неалгебраически построенными подстановками. Демонстрируются отличия в получаемых результатах. Справедливость полученных в работе теоретических результатов проверяется вычислительными экспериментами.

Ключевые слова: AES, дифференциал, дифференциальная характеристика, разность, таблица разности.

ВВЕДЕНИЕ

Таблица 2

В работе [1] был предложен метод оценки максимальной вероятности двухцикловых дифференциалов для Rijndael-подобных шифров. Этот метод, в отличие от аналогичного ранее предложенного метода из [2], не зависит от вида используемых нелинейных подстановок и может быть использован для любых подстановок. Однако в работе [1] было продемонстрировано применение этого метода только для шифров с алгебраически построенными подстановками, которые обладают предельными дифференциальными и линейными показателями. Целью данной работы является демонстрация возможности применения метода из [1] для шифров с произвольными подстановками, каким, например, можно считать шифр «Калина» [3], который стал победителем на украинском конкурсе блочных алгоритмов [4].

1. СУПЕР-S-БЛОКИ AES

Как и в работах [1, 2] будем рассматривать супер-S-блок, который состоит из последовательности операций ByteSub, MixColumns, AddKey и ByteSub и работает с одной колонкой блока данных. Супер-S-блок AES работает с 32-битным блоком, а в настоящей работе мы будем рассматривать 16-битный вариант супер-S-блока, который содержит четыре 4-битных S-блока. Для такого варианта супер-S-блока имеется возможность более подробно изучить свойства в ходе вычислительных экспериментов.

В качестве 4-битовых S-блоков взята произвольно построенная подстановка, представленная в табл. 1.

Таблица 1

Используемая подстановка

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
5	9	B	2	3	6	F	8	7	C	0	E	1	D	4	A

Эта подстановка не является алгебраически построенной и не обладает предельными дифференциальными показателями, что видно из представленной таблицы разностей (см. табл. 2).

Для дальнейших расчетов важным является количество различных значений в этой таблице для случаев, когда входная и выходная разности не равны 0 (см. табл. 3).

Таблица разностей

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	2	0	2	0	2	0	2	4	0	4	0
2	0	0	2	0	0	2	0	4	0	0	2	2	0	4	0	0
3	0	0	2	0	0	0	0	2	0	6	0	4	2	0	0	0
4	0	2	0	0	6	0	4	0	0	0	2	0	0	0	0	2
5	0	0	0	4	0	0	0	0	0	8	0	0	4	0	0	0
6	0	4	0	4	2	0	2	0	2	0	2	0	0	0	0	0
7	0	2	0	0	0	0	2	0	2	0	0	0	8	0	0	2
8	0	0	6	0	0	2	0	0	0	0	6	2	0	0	0	0
9	0	0	2	0	0	4	0	2	0	2	0	0	2	0	4	0
A	0	0	0	0	0	4	0	4	0	0	0	4	0	4	0	0
B	0	0	4	0	0	2	0	2	0	6	0	2	0	0	0	0
C	0	0	0	0	6	0	2	0	2	0	2	0	0	0	0	4
D	0	6	0	0	0	0	2	0	6	0	0	0	0	0	0	2
E	0	2	0	4	2	0	0	0	4	0	2	0	0	0	0	2
F	0	0	0	4	0	0	4	0	0	0	0	0	4	0	4	4

Таблица 3

Статистическая информация для таблицы разности

Значение	Количество значений в таблице разностей
“8”	2
“6”	8
“4”	22
“2”	36
“0”	157

Таким образом, при условии, что входная и выходная разности не равны 0, доля ненулевых значений в таблице разности составляет $68/225=0,3$.

В преобразовании MixColumns (MC) используется матрица вида

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}.$$

2. АНАЛИЗ СУПЕР-S-БЛОКА «СИЛОВЫМ» СПОСОБОМ

Используя полный перебор возможных значений входной пары был определен двухцикловый дифференциал, обладающий максимальной вероятностью $3/128$. Входная разность этого дифференциала 5550, выходная — 00D1. Принадлежит этому дифференциалу только одна

дифференциальная характеристика, которая представлена на рис. 1.

5	5	5	0	
B		S		8 8 8
A	A	A	0	
M		C		
0	0	7	D	
B		S		8 6
0	0	D	1	

Рис. 1

На рис. 1 справа напротив преобразований BS (ByteSubstitution) представлены значения из таблицы разности, на которые попадают указанные переходы разности для отдельных S-блоков, которые содержат на входе ненулевую разность.

Следует заметить, что использовать упомянутый выше полный перебор возможных значений входной пары возможно лишь для супер-S-блока размером до 32 битов. Для супер-S-блоков большего размера, которые, например, используются в шифре «Калина», в шифрующих преобразованиях функций хеширования Whirlpool, Groestl, значение максимальной вероятности можно получить только на основании анализа особенностей шифрующих преобразований. Продемонстрируем как это может быть сделано для рассматриваемого шифра. Для этого будем придерживаться основных этапов предложенного в [1] подхода:

1. Определение минимального количества активных S-блоков.
2. Определение вида ДХ, обладающей максимальной вероятностью.
3. Определение количества и вероятностей дополнительных ДХ.
4. Определение максимальной вероятности двухциклового дифференциала.

В соответствии с числом ветвей активизации (branch number) МДР-преобразования при ненулевой входной разности всегда будет минимум пять активных S-блоков. Возможны различные варианты для количества активных S-блоков на входе и выходе: 1 и 4, 2 и 3, 3 и 2, 4 и 1. Рассмотрим эти варианты.

3. КОЛИЧЕСТВО АКТИВНЫХ S-БЛОКОВ: 1 НА ВХОДЕ, 4 НА ВЫХОДЕ

В табл. 4 представлены 16 вариантов разности на входе в МС и соответствующие значения разности на выходе МС.

Выходные значения для преобразования МС являются входными для второго уровня S-блоков. Как видно из табл. 4, трое из четырех тетрад всегда содержат различную разность. Так как в таблице разности (табл. 2) присутствует только два перехода с вероятностью 8/16, то вероятность того, что для всех четырех активных S-блоков 2-го уровня может быть выполнен переход разности с максимальной вероятностью (8/16) равна 0:

$$P_{1 \rightarrow 4}(4_перехода_разности_с_вероятностью \frac{8}{16}) = 0.$$

Таблица 4

Вход МС	Выход МС
1000	2113
2000	4226
3000	6335
4000	844c
5000	a55f
6000	c66a
7000	e779
8000	388b
9000	1998
A000	7AAD
B000	5BBE
C000	BCC7
D000	9DD4
E000	FEE1
F000	DFE2

Оценим вероятность того, что для всех пяти активных S-блоков может быть выполнен переход разности с вероятностью не менее, чем 6/16. Для этого, сначала, рассмотрим таблицу разности (табл. 3). Из 15 строк и столбцов с ненулевой входной и выходной разностью значения 6 и более присутствуют в 8 строках и 8 столбцах. Поэтому, если считать, что три различных значения разности на втором уровне S-блоков появляются случайно, то вероятность того, что для всех четырех активных S-блоков 2-го уровня может быть выполнен переход разности с вероятностью 6/16 и более равна:

$$P_{1 \rightarrow 4}(4_перехода_разности_с_вероятностью \geq \frac{6}{16}) = \left(\frac{8}{15}\right)^3.$$

Учитывая наличие 8 вариантов разности для активного S-блока первого уровня, когда может быть выполнен переход разности с вероятностью 6/16 и более, ожидаемое количество случаев, когда все 5 переходов разности выполняются с вероятностью 6/16 и более, составит:

$$OK_{1 \rightarrow 4}(5_переходов_разности_с_вероятностью \geq \frac{6}{16}) = 8 \cdot \left(\frac{8}{15}\right)^3 \approx 1.$$

Этот прогноз подтвердили вычислительные эксперименты. Найдена дифференциальная характеристика (ДХ), в которой все 5 переходов разности выполняются с вероятностью 6/16 (см. рис. 2).

Оценим вероятность существования дополнительных ДХ, принадлежащих такому дифференциалу. Дополнительные ДХ должны содержать одинаковые с основной ДХ входную и выходную разности, но другие промежуточные значения разностей.

4	0	0	0	
B		S		6
4	0	0	0	
M		C		
8	4	4	C	
B		S		6666
2	4	4	4	

Рис. 2

Учитывая, что доля ненулевых значений в таблице разности (см. табл. 3) $68/225 = 0,3$, а в каждой строке таблицы разности со значением 6 и более в среднем присутствует 3 других ненулевых значения, то ожидаемое количество дополнительных ДХ составит:

$$OK_{1 \rightarrow 4}(\text{дополнительных_ДХ}) = 3 \cdot 0,3^3 = 0,081,$$

следовательно, очень маловероятно наличие дополнительных ДХ, что также подтвердили вычислительные эксперименты.

В значительно меньшем количестве дополнительных ДХ состоит главное отличие шифрующего преобразования с произвольными подстановками от преобразования с алгебраически построенными подстановками с предельными дифференциальными и линейными показателями.

4. КОЛИЧЕСТВО АКТИВНЫХ S-БЛОКОВ: 2 НА ВХОДЕ, 3 НА ВЫХОДЕ

В случае, когда на входе в МС 2 активных тетрады, то только при определенном соотношении разности в этих тетрадах на выходе МС может быть получена нулевая разность в одной из четырех тетрад. Например, для получения нулевой разности в третьей тетраде на выходе МС две первые тетрады на входе в МС должны содержать одинаковое значение разности (см. примеры на рис. 3).

7	7	0	0			5	5	0	0		
	B	S		88			B	S		88	
D	D	0	0			A	A	0	0		
	M	C					M	C			
D	4	0	9			A	D	0	7		
	B	S		664			B	S		468	
1	4	0	5			5	1	0	D		

Рис. 3

В любом случае, из 5 активных S-блоков в трех всегда будет различная разность, а следовательно, в соответствии с табл. 3, все пять переходов разности с вероятностью $8/16$ произойти не могут.

Вернемся к рассматриваемому варианту прохождения разности, когда две первые тетрады на входе в МС содержат одинаковое значение разности и нулевая разность в третьей тетраде на выходе МС. Вероятность того, что 3 перехода разности на втором уровне S-блоков могут быть выполнены с вероятностью $6/16$ и более:

$$P_{2 \rightarrow 3}(3_перехода_разности_с_вероятностью \geq \frac{6}{16}) = \left(\frac{8}{15}\right)^3 = 0,15.$$

Учитывая наличие 8 вариантов разности для двух активных S-блоков первого уровня, содержащих одинаковую разность, когда может быть выполнен переход разности с вероятностью $6/16$ и более, ожидаемое количество случаев, когда все 5 переходов разности выполняются с вероятностью $6/16$ и более, составит:

$$OK_{2 \rightarrow 3}(5_переходов_разности_с_вероятностью \geq \frac{6}{16}) = 8 \cdot \left(\frac{8}{15}\right)^3 \approx 1.$$

При этом последняя оценка справедлива для каждого отдельного варианта расположения тетрады с нулевой разностью на выходе преобразования МС. Так как есть 4 варианта такого расположения, то можно ожидать такое же количество различных ДХ при фиксированной позиции входных активных S-блоков.

На рис. 4, а представлена ДХ с вероятностью всех переходов $6/16$ и более и третьей нулевой тетрадой на выходе МС, а на рис. 4, б представлена ДХ с вероятностью всех переходов $6/16$ и более и второй нулевой тетрадой на выходе МС.

4	4	0	0			3	7	0	0		
	B	S		66			B	S		68	
4	4	0	0			9	D	0	0		
	M	C					M	C			
4	C	0	8			5	0	4	5		
	B	S		666			B	S		868	
4	4	0	2			A	0	4	A		

Рис. 4

Для каждой такой ДХ ожидаемое количество дополнительных ДХ рассчитывается также как и в предыдущем разделе и составляет:

$$OK_{2 \rightarrow 3}(\text{дополнительных_ДХ}) = 3 \cdot 0,3^3 = 0,081.$$

5. КОЛИЧЕСТВО АКТИВНЫХ S-БЛОКОВ: 3 НА ВХОДЕ, 2 НА ВЫХОДЕ

В случае, когда на входе в МС 3 активных тетрады, то только при определенном соотношении разности в этих тетрадах на выходе МС может быть получена нулевая разность в двух из четырех тетрад. Например, для получения нулевой разности в первой и во второй тетрадах на выходе МС три первые тетрады на входе в МС должны содержать одинаковое значение разности (см. пример на рис. 5).

7	7	7	0		
	B	S		888	
D	D	D	0		
	M	C			
0	0	9	4		
	B	S		46	
0	0	5	4		

Рис. 5

При этом для дальнейших оценок важно, что значения в активных тетрадах на выходе МС будут всегда разные. Оценим вероятность того, что из этих двух различных значений разности будут возможны переходы с вероятностью $8/16$.

$$P_{3 \rightarrow 2}(2_перехода_разности_с_вероятностью \geq \frac{8}{16}) = \frac{2}{15} \cdot \frac{1}{15} \approx 0,009.$$

Тогда ожидаемое количество случаев, когда все 5 переходов разности произойдут с вероятностью $8/16$:

$$OK_{3 \rightarrow 2}(5_переходов_разности_с_вероятностью \geq \frac{8}{16}) = 2 \cdot \frac{2}{15} \cdot \frac{1}{15} \approx 0,018.$$

Вычислительные эксперименты подтвердили отсутствие таких случаев.

Вероятность того, что для двух активных тетрад на выходе МС будут существовать переходы с вероятностью 6/16 и больше, будет значительно выше:

$$P_{3 \rightarrow 2}(2_перехода_разности_с_вероятностью \geq \frac{6}{16}) = \frac{8}{15} \cdot \frac{7}{15} \approx 0,25.$$

Ожидаемое количество случаев, когда все 5 переходов разности произойдут с вероятностью 6/16 и более составит

$$OK_{3 \rightarrow 2}(5_переходов_разности_с_вероятностью \geq \frac{6}{16}) = 8 \cdot \frac{8}{15} \cdot \frac{7}{15} \approx 2.$$

Эти случаи представлены на рис. 6.

5	5	5	0		4	4	4	0	
	B	S		888		B	S		666
a	A	A	0		4	4	4	0	
	M	C				M	C		
0	0	7	D		0	0	8	C	
	B	S		86		B	S		66
0	0	d	1		0	0	2	4	

Рис. 6

Ожидаемое количество дополнительных ДХ:

$$OK_{3 \rightarrow 2}(\text{дополнительных_ДХ}) = 3 \cdot 0,3^2 = 0,27.$$

Вариант с четырьмя активными S-блоками на входе и 1 на выходе идентичен варианту с переходом 1 в 4 и поэтому рассматривать отдельно не будем.

ВЫВОДЫ

1. Определена максимальная вероятность для двухцикловых дифференциалов для рассматриваемого 16-битного супер-S-блока, в котором используется произвольная подстановка. Эта вероятность $1536/2^{16}$, что значительно больше, чем та же вероятность для случая с алгебраически построенными подстановками — $72/2^{16}$. Этот результат вполне ожидаем, т. к. произвольная подстановка обладает в два раза более высокой максимальной вероятностью прохождения ненулевой разности.

2. Определен вид обладающего максимальной вероятностью дифференциала, который отличается от аналогичного дифференциала, найденного в [1].

3. Одно из главных отличий шифрующего преобразования с произвольными подстановками от преобразования с алгебраически построенными подстановками с предельными дифференциальными и линейными показателями состоит в том, что для всех рассмотренных дифференциалов было найдено значительно меньшее количество дополнительных ДХ (все рассмотренные дифференциалы состояли из одной ДХ).

4. Еще одной обнаруженной особенностью стало отсутствие среди рассмотренных дифференциалов таких, вероятность которых изменялась бы для разных ключей.

5. По-прежнему актуальным остается вопрос получения точных значений вероятностей дифференциалов с большим размером блока и большим количеством циклов.

Литература

- [1] Руженцев В.И. Оценка вероятностей двухцикловых дифференциалов шифра AES / В.И. Руженцев // Прикладная радиоэлектроника. — 2011. — № 2. — Т. 10. — С. 116–121.
- [2] J.Daemen, V. Rijmen. Two-Round AES Differentials. IACR Eprint archive, 2006. available from <http://eprint.iacr.org/2006/039>.
- [3] Перспективний блоковий симетричний шифр “Калина” — основні положення та специфікація / І. Д. Горбенко, В. І. Долгов, Р. В. Олійников, В. І. Руженцев та ін. // Прикладна радиоелектроніка. Тематический випуск, посвящений проблемам забезпечення безпеки інформації. Харків. Том 6, № 2, 2007. — С. 195–208.
- [4] Офіційний ресурс департаменту спеціальних телекомунікаційних систем та захисту інформації: «Положення про проведення відкритого конкурсу криптографічних алгоритмів», 2006. Доступно по адресу <http://www.dststz.gov.ua/dststz/control/ru/publish/article/>.



Поступила в редколлегию 22.08.2014

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ, ХНУРЭ. Научные интересы: криптография, криптоанализ блочных симметричных шифров

УДК 004.056.55

Ймовірності двоциклових диференціалів Rijndael-подібних шифрів з довільними підстановками / В.І. Руженцев // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 235–238.

Робота присвячена аналізу двоциклових диференціалів Rijndael-подібних шифрів. Запропонований в попередній роботі підхід щодо оцінки ймовірностей диференціалів застосовується для шифрів з неалгебраїчно побудованими підстановками. Демонструються відмінності в отриманих результатах. Слушність отриманих теоретичних висновків перевіряється обчислювальними експериментами.

Ключові слова: AES, диференціал, диференціальна характеристика, різниця, таблиця різниці.

Табл.: 4. Іл.: 6. Бібліогр.: 4 найм.

UDC 004.056.55

The probabilities of two-round differentials for Rijndael-like ciphers with random substitutions / V.I. Ruzhentshev // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 235–238.

The paper is devoted to analyzing two-round differentials of Rijndael-like ciphers. The approach to estimating differential probabilities, which was suggested in one of the previous works, is used for ciphers with nonalgebraically formed substitutions. The main differences in the results obtained are demonstrated. The theoretical results are then compared with results of computing experiments.

Keywords: AES, differential, differential characteristic, difference, difference table.

Tab.: 4. Fig.: 6. Ref.: 4 items.

ПЕРІОДИЧНІ ВЛАСТИВОСТІ ШИФРГАМИ У РЕЖИМІ OUTPUT FEEDBACK*О.О. КУЗНЕЦОВ, Ю.І. ГОРБЕНКО, Є.П. КОЛОВАНОВА*

Досліджуються властивості режиму гамування зі зворотним зв'язком за шифрґамою (англомовне позначення – Output Feedback). Із застосуванням математичного апарату теорії підстановок досліджуються періодичні властивості ґами, зокрема проводиться оцінка ймовірності появи ґами певного періоду за умови відповідності властивостей блокового симетричного шифру певним властивостям випадкової підстановки. Розробляються практичні рекомендації щодо застосування режиму гамування зі зворотним зв'язком за шифрґамою, обґрунтовуються вимоги та обмеження, що випливають із отриманих оцінок періодичних властивостей ґами.

Ключові слова: режим шифрування, періодичність ґами, випадкова підстановка, Output Feedback.

ВСТУП

Для забезпечення інформаційної безпеки в умовах реальних та потенційних загроз, зокрема, від несанкціонованого доступу до інформаційних ресурсів, у тому числі, внаслідок використання іноземних інформаційних технологій, Адміністрацією Держспецзв'язку України ініційовано розробку вітчизняного криптографічного алгоритму симетричного блокового перетворення [1, 2]. Його призначено для забезпечення взаємної сумісності засобів криптографічного захисту інформації різних виробників, що застосовуються для вирішення завдань конфіденційності, цілісності та інших послуг безпеки, у тому числі для захисту публічної інформації, яка обробляється та циркулює в інформаційно-телекомунікаційних системах.

Специфікацію нового алгоритму симетричного блокового криптоперетворення визначено у проекті національного стандарту ДСТУ “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення” [1, 2], в якому передбачено можливість забезпечення конфіденційності та цілісності повідомлення шляхом послідовного застосування відповідних перетворень. Однак властивості криптоперетворень залежать не тільки від характеристик шифру, але й від режимів його застосування. Тому у проекті стандарту передбачено 10 режимів криптоперетворення: проста заміна (базове перетворення), гамування, гамування зі зворотним зв'язком за шифр-текстом, вироблення імітовставки, зчеплення шифрблоків, гамування зі зворотним зв'язком за шифрґамою, вибіркове гамування із прискореним виробленням імітовставки, вироблення імітовставки і гамування, індексованої заміни, захисту ключових даних [1, 2].

Одним із найбільш поширених режимів блокового симетричного шифрування, який застосовується для забезпечення послуги конфіденційності, є режим гамування зі зворотним зв'язком за шифрґамою (в англійських виданнях застосовується позначення Output Feedback – OFB). У цьому режимі вихідне повідомлення не підлягає криптоперетворенню, тобто не шифрується

у звичайному розумінні. Конфіденційність повідомлення забезпечується шляхом додавання до нього шифрґами, яка формується багаторазовим шифруванням одного й того самого несекретного блоку ініціалізації (у вітчизняній термінології застосовується поняття синхропосилки). На приймальній стороні знову формується шифрґама, дію якої знімають з криптограми.

Таким чином, режим OFB має кілька переваг: по-перше, шифрґама може бути сформована заздалегідь, ще до появи повідомлення, внаслідок чого можна значно прискорити процес захисту інформації; по-друге, в цьому режимі, як і в режимі простої заміни (Electronic Codebook – ECB), помилки, що можуть виникнути при передачі шифротексту по каналах зв'язку, локалізуються в блоці, не поширюючись на сусідні, причому в режимі OFB помилковими будуть лише біти, які підлягали зміні (в режимі ECB зміниться весь блок); по-третє, криптографічні властивості шифрґами не залежать від відкритого тексту, вони визначаються лише властивостями базового криптоперетворення, та, можливо, значенням блоку ініціалізації (синхропосилки), який і визначає конкретний вигляд та періодичність ґами. Саме вивченню періодичних властивостей шифрґами у режимі OFB і присвячена ця робота, адже виникнення повторення ґами є найбільш небезпечним випадком, що дає зловмисникові можливість порушити встановлений режим конфіденційності повідомлень.

Робота структурована наступним чином. У розділі 2 наводиться опис режиму гамування зі зворотним зв'язком за шифрґамою. При викладенні режиму застосовується термінологія і основні позначення з проекту національного стандарту ДСТУ “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення” [1, 2]. У розділі 3 вивчається зв'язок предмета дослідження із загальними положеннями теорії підстановок [3–5], зокрема, вводяться основні поняття та визначення, які пов'язуються із певними властивостями симетричних блокових криптоперетворень, наводяться основні аналітичні співвідношення, які застосовуються в ході вивчення

випадкових підстановок, зокрема, відомі розподіли кількості циклів, зростають та інверсій тощо. Розділ 4 присвячено викладенню основних теоретичних результатів, отриманих в цій роботі. Зокрема, із застосуванням розподілів кількостей циклів певної довжини випадкової підстановки виводиться формула для оцінки ймовірності появи циклу для довільного фіксованого значення множини перетворень. Ця властивість має безпосереднє відношення до періодичних властивостей шифрґрами, бо характеризує ймовірнісний розподіл появи гам певного періоду за умови виконання припущення щодо відповідності властивостей блокового симетричного шифру (БСШ) певним властивостям випадкової підстановки. У розділі 5 наводиться докладний приклад розрахунку ймовірностей появи циклу заданої довжини у випадково обраній підстановці, тобто в цьому розділі на прикладі з докладними поясненнями демонструється справедливості отриманої формули та наведених комбінаторних міркувань. Розділ 6 присвячено інтерпретації отриманих результатів щодо вивчення властивостей блокових шифрів, зокрема, наводяться результати оцінки ймовірності появи шифрґрами з різною довжиною періоду. Також у цьому розділі вирішуються конкретні практичні задачі, а саме розробляються рекомендації щодо застосування режиму гамування зі зворотним зв'язком за шифрґрамою, обґрунтовуються певні вимоги та обмеження. У висновках узагальнюються та конкретизуються отримані результати, обговорюються можливі шляхи подальших досліджень.

1. РЕЖИМ ГАМУВАННЯ ЗІ ЗВОРОТНИМ ЗВ'ЯЗКОМ ЗА ШИФРґРАМОЮ

Режим гамування зі зворотним зв'язком за шифрґрамою призначено для забезпечення послуги конфіденційності. Цей режим засновано на шифруванні вектора ініціалізації (синхропосилки) для генерації послідовності вихідних блоків (шифрґрами), які додаються до звичайного тексту, щоб сформувати зашифрований текст і, навпаки, до шифртексту для його розшифрування. Режим вимагає, аби вектор ініціалізації (синхропосилка) був унікальним для кожного застосування із наданим (фіксованим) ключем. Розглянемо специфікацію режиму гамування зі зворотним зв'язком за шифрґрамою, яку наведено у проекті національного стандарту БСШ «Калина» [1, 2].

Відповідно до специфікації режим гамування зі зворотним зв'язком за шифрґрамою позначається як Калина- l/k -OFB. Він забезпечує конфіденційність повідомлення шляхом шифрування. Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C , $|C| = |M|$, та обернене відображення шифртексту C у повідомлення M . Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються. Параметрами

режиму є ключ шифрування K , $|K| = k$ та синхропосилка S , $|S| = l$. Додаткові вимоги щодо синхропосилки не накладаються.

В ході зашифрування повідомлення M ($|M| \geq 1$) подається у вигляді послідовності блоків:

$$M = m_1 \| m_2 \| \dots \| m_n, |m_i| = l,$$

для $i = 1, 2, \dots, n-1$, $1 \leq m_n \leq l$.

Початкове значення блока гами γ_0 ($|\gamma_0| = l$) обчислюється як

$$\gamma_0 = T_{l,k}^{(K)}(S). \quad (1)$$

Кожен з блоків шифртексту обчислюється відповідно до співвідношення

$$c_i = m_i \oplus L_{l,|m_i|}(\gamma_{i-1}), \quad (2)$$

для $i = 1, 2, \dots, n$, та

$$\gamma_i = T_{l,k}^{(K)}(\gamma_{i-1}), \quad (3)$$

для $i = 1, 2, \dots, n-1$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \| c_2 \| \dots \| c_n$.

В ході розшифрування шифртексту C ($|C| \geq 1$) подається у вигляді послідовності блоків:

$$C = c_1 \| c_2 \| \dots \| c_n, |c_i| = l$$

для $i = 1, 2, \dots, n-1$, $1 \leq c_n \leq l$.

Початкове значення блока гами γ_0 ($|\gamma_0| = l$) обчислюється як

$$\gamma_0 = T_{l,k}^{(K)}(S).$$

Кожен з блоків повідомлення обчислюється відповідно до співвідношення

$$m_i = c_i \oplus L_{l,|m_i|}(\gamma_{i-1}), \quad (4)$$

для $i = 1, 2, \dots, n$, та

$$\gamma_i = T_{l,k}^{(K)}(\gamma_{i-1}),$$

для $i = 1, 2, \dots, n-1$.

Результатом розшифрування шифртексту є повідомлення $M = m_1 \| m_2 \| \dots \| m_n$.

Схему зашифрування та розшифрування у режимі гамування зі зворотним зв'язком за шифрґрамою наведено на рис. 1. Ця схема формально зображує послідовність виконання перетворень (2), (4) за всіма значеннями циклової змінної $i = 1, 2, \dots, n$.

Розглянемо періодичність гами у режимі гамування зі зворотним зв'язком за шифрґрамою. Перш за все відзначимо, що, за визначенням, гама складається із початкового значення блоку γ_0 та решти блоків γ_i , які обчислюються за (1), (3) для кожного значення циклової змінної $i = 1, 2, \dots, n-1$. Тобто, задача дослідження полягає саме у визначенні періоду послідовності блоків γ_i , $i = 0, 1, \dots, n-1$.

Кожен блок гами γ_i є результатом зашифрування попереднього блоку γ_{i-1} , де початкове значення γ_0 дорівнює результату зашифрування синхропосилки. Якщо скористатися термінологією теорії підстановок [3–5] і представити базове шифрувальне перетворення $T_{l,k}^{(K)}$, ініці-

йоване секретним ключем K , як деяку підстановку s , що діє на множині відкритих текстів, тоді період послідовності блоків шифрми $\gamma_0, \gamma_1, \dots, \gamma_{n-1}$ відповідатиме одному із циклів $s_i = (y, s_i(y), s_i^2(y), \dots, s_i^{l_i-1}(y))$ підстановки s , де початкове значення циклу y дорівнює значенню синхросилки S .

Кожен наступний елемент $s_i^j(y)$ циклу s_i довжини l_i є результатом багаторазового зашифрування синхросилки:

$$\begin{aligned} y &= S; \\ s_i(y) &= T_{l,k}^{(K)}(S) = \gamma_0; \\ s_i^2(y) &= T_{l,k}^{(K)}(T_{l,k}^{(K)}(S)) = \gamma_1; \\ &\dots \\ s_i^{l_i-1}(y) &= \underbrace{T_{l,k}^{(K)}(T_{l,k}^{(K)} \dots T_{l,k}^{(K)}(S))}_{l_i-1 \text{ разів}} = \gamma_{l_i-2}; \\ s_i^{l_i}(y) &= \underbrace{T_{l,k}^{(K)}(T_{l,k}^{(K)} \dots T_{l,k}^{(K)}(S))}_{l_i \text{ разів}} = \gamma_{l_i-1} = \gamma_0; \\ &\dots \\ s_i^n(y) &= \underbrace{T_{l,k}^{(K)}(T_{l,k}^{(K)} \dots T_{l,k}^{(K)}(S))}_{n \text{ разів}} = \gamma_{n-1}. \end{aligned}$$

Таким чином, дослідження періодичних властивостей послідовності блоків шифрми $\gamma_i, i=0,1,\dots,n$ полягає у вивченні циклової структури підстановки s , а саме в оцінці розподілу довжин l_i циклів s_i для різних початкових значень $y=S$ базового шифрувального перетворення $T_{l,k}^{(K)}$. Такі дослідження дадуть змогу оцінити довжину періоду l_i шифрми для різних $y=S$ та

K або визначити ймовірність формування гами певного періоду для довільного фіксованого значення синхросилки $y=S$ та випадково обраного секретного ключа K .

Розглянемо окремі положення теорії підстановок та їх зв'язок із властивостями БСШ, зокрема, введемо основні поняття та визначення, які пов'язані з певними властивостями симетричних блокових криптоперетворень (розподіли кількості циклів, зростань та інверсій тощо).

3. ОКРЕМІ ПОЛОЖЕННЯ ТЕОРІЇ ПІДСТАНОВОК ТА ЇХ ЗВ'ЯЗОК ІЗ БСШ

За визначенням БСШ «Калина» (його базове перетворення $T_{l,k}^{(K)}$) є параметризованою ключем K функцією бієктивного відображення множини відкритих текстів у множину шифртекстів: $V_l \rightarrow V_l, K \in V_k, l, k \in \{128, 256, 512\}$ [1, 2]. Загалом, для довільного l -бітового блокового шифру існує $2^l!$ можливих перестановок відкритого тексту. Ці перетворення, які мають назву підстановок степеня 2^l , утворюють групу відносно операції послідовного виконання перетворень. Така група має назву симетричної групи підстановок степеня 2^n та позначається як S_{2^l} [3]. Практично це означає, що кількість бітів ключа, яку необхідно для отримання всіх можливих перестановок, становить близько $\ln 2^l! \approx l \cdot 2^l$ бітів¹. Однак розмір ключа алгоритму «Калина» приймає значення у 128, 256 або 512 біт, тобто використовується лише невелика частка від повної кількості можливих перестановок. Наприклад, для $l = 128$ ма-

¹ За формулою Стірлінга $\ln(x!) = x \ln(x) - x - O(\ln(x))$

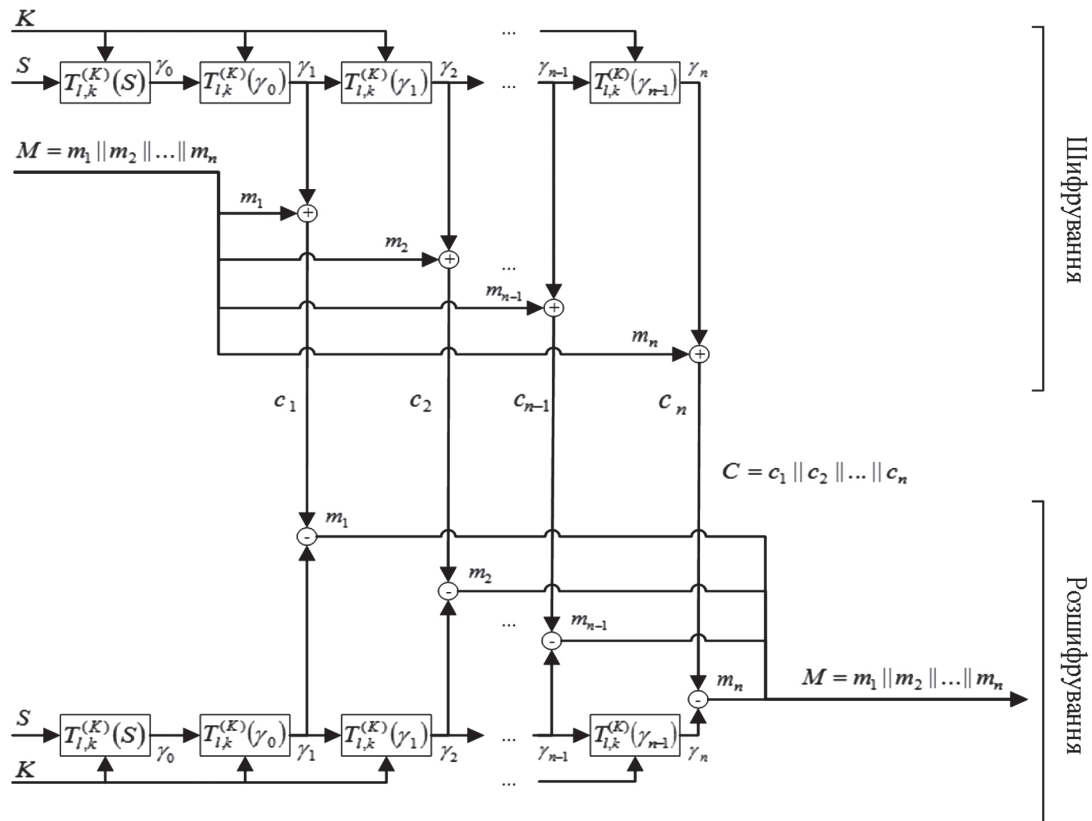


Рис. 1. Схема зашифрування та розшифрування у режимі гамування зі зворотним зв'язком за шифрною

емо $2^{128}! \approx 2^{128 \cdot 2^{128}}$ можливих перестановок 128-бітових блоків, з яких, залежно від довжини ключа, використовуються тільки 2^{128} або 2^{256} перетворень². Таким чином, базове перетворення шифру є по суті деякою підмножиною повної множини всіх можливих підстановок, що діють на множині блоків оброблюваних даних. Основне припущення, яке приймається в ході обґрунтування стійкості симетричного криптоперетворення полягає саме у збереженні ймовірнісних властивостей випадкової підстановки. Тобто припускається, що хоча при шифруванні й застосовується обмежений набір підстановок із S_{2^l} , однак певні розподіли ймовірностей елементів цієї підмножини відповідають властивостям випадково обраної підстановки із всієї множини S_{2^l} [6–9].

Розглянемо основні поняття та визначення теорії підстановок [3] та пов'яжемо їх із цикловими властивостями БСШ. Для цього розглянемо множину всіх бієктивних перетворень множини $Y = \{y_1, y_2, \dots, y_n\}$ саму в себе, що утворюють симетричну групу S_n потужності $n!$ всіх можливих підстановок степеня n . За визначенням симетричної групи [3], кожній підстановці $s \in S_n$ відповідає єдина підстановка $s^{-1} \in S_n$, така, що

$$s^{-1} \cdot s(y) = s \cdot s^{-1}(y) = e(y), \quad y \in Y,$$

де $e(y) \in S_n$ — одинична підстановка, тобто $e(y) = y$ для всіх $y \in Y$.

Скористаємося позначеннями:

$$s \cdot s \cdot \dots \cdot s = s^k, \quad s^{-1} \cdot s^{-1} \cdot \dots \cdot s^{-1} = s^{-k},$$

де добутки містять k множників.

Відповідно маємо

$$s^k \cdot s^{-k} = s^{-k} \cdot s^k = s^0 = e.$$

Множина підстановок степеня n , яка є замкнутою відносно операції множення та обчислення оберненого для $s \in S_n$ елементу $s^{-1} \in S_n$, має назву групи підстановок. Кожна така група є підгрупою симетричної групи S_n [3].

Розглянемо деяку підстановку $s \in S_n$, яка діє на множині Y . Визначимо на множині Y бінарне відношення, при цьому вважатимемо $y \sim y'$ для $y, y' \in Y$ якщо існує таке j , що $y' = s^j(y)$. Це бінарне відношення є рефлексивним, симетричним та транзитивним, тобто є відношенням еквівалентності. Дійсно, відповідно до [3] маємо:

— $y \sim y$, оскільки $y = s^0(y) = e(y)$;

— із умови $y \sim y'$ випливає $y' \sim y$, оскільки із

рівності $y' = s^j(y)$ випливає, що $y = s^{-j}(y')$;

— із $y \sim y'$ та $y' \sim y''$ випливає, що $y \sim y''$, бо з рівностей $y' = s^j(y)$ та $y'' = s^l(y')$ випливає, що $y'' = s^i(s^j(y)) = s^{i+j}(y)$.

Цикл s_i підстановки $s \in S_n$ довжини l_i визначається так:

$$s_i = (y, s_i(y), s_i^2(y), \dots, s_i^{l_i-1}(y)),$$

де $s_i^{l_i}(y) = y$.

² Відповідно до специфікації алгоритму «Калина» для $l = 128$ відповідне k може дорівнювати 128 або 256

Довільну підстановку $s \in S_n$ можна розкласти на відповідні цикли [3]:

$$s = (y_1, s_1(y_1), s_1^2(y_1), \dots, s_1^{l_1-1}(y_1)) \dots \\ \dots (y_k, s_k(y_k), s_k^2(y_k), \dots, s_k^{l_k-1}(y_k)). \quad (5)$$

Елементи y_i та y_{i+1} в підстановці $s \in S_n$ утворюють зростання, якщо $s(y_i) > s(y_{i+1})$, при цьому приймається, що елементу y_1 завжди передують зростання. Пара елементів y_i та y_j в підстановці $s \in S_n$ утворює інверсію, якщо $s(y_i) > s(y_j)$, $i < j$.

Наприклад, підстановка s степеня 4-го виду

$$s = \begin{pmatrix} y_1 & y_2 & y_3 & y_4 \\ s(y_1) & s(y_2) & s(y_3) & s(y_4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

може бути подана у вигляді розкладу на 3 цикли:

$$s_1 = (y_1) = (1), \quad l_1 = 1;$$

$$s_2 = (y_2, s_2(y_2)) = (2, 4), \quad l_2 = 2;$$

$$s_3 = (y_3) = (3), \quad l_3 = 1,$$

Тобто, маємо такий розклад:

$$s = (y_1)(y_2, s_2(y_2))(y_3) = (1)(2, 4)(3).$$

У цій підстановці є два зростання (елементу $y_1 = 1$ завжди передують одне зростання, та ще одне зростання утворюють елементи $y_1 = 1$ і $y_2 = 2$, бо $s(y_1) = 1 > s(y_2) = 4$) і три інверсії (їх утворюють пари елементів y_2 та y_3 , y_2 та y_4 , y_3 та y_4 , бо виконуються нерівності $s(y_2) > s(y_3)$, $s(y_2) > s(y_4)$, $s(y_3) > s(y_4)$, відповідно).

На множині всіх підстановок симетричної групи S_n задамо рівномірний ймовірнісний розподіл, тобто кожній вибраній підстановці $s \in S_n$ поставимо у відповідність ймовірність її обрання, що дорівнює $1/n!$. За сучасними поглядами симетричної криптографії така множина рівноймовірних відображень відповідає уявленню про «ідеальний» шифр. Адже, якщо випадкове обрання окремої підстановки $s \in S_n$ пов'язати з значенням введеного ключа шифрування, тоді отримане перетворення відповідатиме випадковому і рівномірно вибраному шифртексту для кожного відкритого тексту при будь-якому ключі, тобто на всіх можливих варіантах відображень відкритого тексту у шифрограмму.

Проведемо дослідження ймовірнісних властивостей випадкової підстановки, зокрема, ймовірностей появи циклу певної довжини у випадково обраній підстановці, бо саме ця подія відповідатиме випадку, коли для довільного фіксованого значення синхропосилки S буде сформована гама γ_i певного періоду.

4. ОЦІНКА ЙМОВІРНОСТІ ПОЯВИ ЦИКЛУ ПЕВНОЇ ДОВЖИНИ У ВИПАДКОВО ОБРАНІЙ ПІДСТАНОВЦІ

Розглянемо випадкову величину ξ_n , яка дорівнює числу циклів у випадково вибраній підстановці $s \in S_n$. Підстановка $s \in S_n$ належить до циклового класу $\{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}\}$, якщо вона містить α_1 циклів довжини 1, α_2 циклів довжини 2 і т. д., тобто:

$$s = (y_1)(y_2) \dots (y_{\alpha_1})(y'_1, y''_1)(y'_2, y''_2) \dots (y'_{\alpha_2}, y''_{\alpha_2}) \dots, \\ 1\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n.$$

Позначимо через $C(\alpha_1, \alpha_2, \dots, \alpha_n)$ число підстановок у цикловому класі $\{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}\}$, а через $C(n, k)$ – число підстановок степеня n , які мають k циклів. Тоді маємо [3]:

$$C(\alpha_1, \alpha_2, \dots, \alpha_n) = \frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!}, \\ C(n, k) = \sum_{\substack{1\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n \\ \alpha_1 + \alpha_2 + \dots + \alpha_n = k, \alpha_i \geq 0}} \frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!} = |s(n, k)|, \quad (6)$$

де $s(n, k)$ – числа Стірлінга першого роду, які визначаються через співвідношення³:

$$(x)_n = x(x-1) \dots (x-n+1) = \sum_{k=0}^n s(n, k) x^k.$$

З формули (6) безпосередньо випливає вираз для точного розподілу ймовірності випадкової події $\xi_n = k$, тобто такого випадку, коли у випадково вибраній підстановці спостерігатиметься точно k циклів (див. вираз (5)).

Скориставшись формулою для обчислення чисел Стірлінга першого роду, маємо [3]:

$$P(\xi_n = k) = \frac{C(n, k)}{n!} = \frac{|s(n, k)|}{n!}, \quad k = 0, 1, \dots, n.$$

В роботі [3] отримано математичне очікування $M\xi_n$ та дисперсію $D\xi_n$ випадкової величини ξ_n :

$$M\xi_n = \sum_{j=1}^n \frac{1}{j} = \ln n + C + o(1),$$

$$D\xi_n = \sum_{j=1}^n \frac{1}{j^2} - \left(\sum_{j=1}^n \frac{1}{j} \right)^2 = \ln n + C + o(1), \quad C = 0,5772 \dots,$$

крім того показано, що при $n \rightarrow \infty$ випадкова величина $\xi'_n = (\xi_n - \ln n) / (\ln n)$ розподілена асимптотично нормально з параметрами $(0, 1)$, тобто

$$\lim_{n \rightarrow \infty} P(\xi'_n < u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^u e^{-y^2/2} dy.$$

Для випадкових величин ζ_n та η_n , які дорівнюють числу зростань та інверсій у випадково обраній підстановці $s \in S_n$, відповідні математичні очікування та дисперсії мають вигляд [3]:

$$M\zeta_n = \frac{n(n-1)}{4}, \quad D\zeta_n = \frac{2n^3 + 3n^2 - 5n}{72},$$

$$M\eta_n = \frac{n}{2}, \quad D\eta_n = \frac{n}{12},$$

при цьому випадкові величини

$$\zeta'_n = (\zeta_n - M\zeta_n) / (D\zeta_n) \quad \text{і} \quad \eta'_n = (\eta_n - M\eta_n) / (D\eta_n)$$

при $n \rightarrow \infty$ також розподілені асимптотично нормально з параметрами $(0, 1)$.

В роботах [6, 9] досліджено емпіричні розподіли ймовірності виникнення певного числа циклів, зростань та інверсій у випадково обраній

³ $(x)_n = x(x-1) \dots (x-n+1)$ – загальноприйняте позначення спадаючого факторіалу (символ Похгаммера)

підстановці із деякої підмножини $V \subset S_n$, елементами якої є підстановки, що реалізуються застосуванням шифрувальної функції на зменшених моделях шифрів⁴. Встановлено, що отримані емпіричні розподіли дуже близькі до розглянутих теоретичних розподілів, тобто можна стверджувати, що зменшені моделі БСШ за цими критеріями подібні властивостям випадкової підстановки із S_n .

Водночас, для оцінки ймовірності формування шифрами γ_i певного періоду для довільного фіксованого значення синхросилки S потрібна інша характеристика випадкової підстановки, а саме розподіл числа циклів заданої довжини. Відповідно до [3], ця характеристика у випадковій підстановці визначається наступним чином.

Позначимо як $\chi_{n,L}$ число циклів довжини L у випадковій рівномірноюбраній підстановці степеня n . Очевидно, що

$$\xi_n = \chi_{n,L=1} + \chi_{n,L=2} + \dots + \chi_{n,L=n}.$$

Розподіл ймовірностей випадкової події $\chi_{n,L} = k$ визначається як [3]:

$$P(\chi_{n,L} = k) = \frac{1}{L^k k!} \sum_{j=0}^{[n/L]-k} \frac{(-1)^j}{L^j j!}, \quad k = 0, 1, \dots, [n/L]. \quad (7)$$

При $n \rightarrow \infty$ випадкова величина $\chi_{n,L}$ має в межі розподіл Пуассона з параметрами $\lambda = 1/L$, тобто

$$\lim_{n \rightarrow \infty} P(\chi_{n,L} = k) = \frac{1}{L^k k!} e^{-1/L}, \quad k = 0, 1, \dots \quad (8)$$

Скористаємося формулою точного розподілу ймовірностей випадкової події $\chi_{n,L} = k$ у вигляді (7) [3]. Значення $n!P(\chi_{n,L} = k)$ відповідає кількості підстановок, які містять k циклів довжини L . Нас цікавить кількість таких підстановок $s \in S_n$, які для довільного фіксованого $y_i \in Y$ обов'язково матимуть цикли $s_i = (y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{l_i-1}(y_i))$ довжини $L = l_i$. Розглянемо випадок, коли $L = 1$, тобто підраховуємо кількість таких підстановок із S_n , які для довільного фіксованого $y_i \in Y$ обов'язково матимуть цикл (y_i) довжини $L = l_i = 1$. У криптографії при розгляді блокових симетричних шифрів розтворення такі випадки прийнято називати фіксованими точками підстановки [6].⁵

З урахуванням $L = 1$, формула (7) набуде вигляду

⁴ Обрання підстановки полягало у випадковому обранні ключа шифрування, який параметризує шифрувальну функцію і задає конкретний вигляд відображення (підстановку) множини відкритих текстів у множину шифртекстів. При цьому застосовувалися зменшені (16-бітні) моделі шифрів, що реалізують деяку підмножину $V \subset S_{2^{16}}$ підстановок 16-бітних векторів

⁵ Тут ідеться тільки про підстановки, які містять лише конкретну фіксовану точку (цикл) (y_i) , яка відповідає обраному $y_i \in Y$. Зазвичай у відомих джерелах оцінюється загальна кількість підстановок, які містять будь-яку фіксовану точку (y_i) для довільного $i = 1, 2, \dots, n$ на повній множині Y із n елементів

$$P(\chi_{n,L=1} = k) = \frac{1}{k!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!}, \quad k = 0, 1, \dots, n,$$

причому для кожного $k = 1, \dots, n$ кожен з $n!P(\chi_{n,L=1} = k)$ випадків для довільного фіксованого $y_i \in Y$ спостерігатиметься точно

$$\frac{C_{n-1}^{k-1}}{C_n^k} = \frac{(n-1)!}{(k-1)!(n-k)!} \frac{k!(n-k)!}{n!} = \frac{k}{n} \quad (9)$$

разів, тобто кількість підстановок, що містять одну фіксовану точку конкретного вигляду (цикл (y_i)) визначатиметься за формулою:

$$\sum_{k=1}^n n!P(\chi_{n,L=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = \sum_{k=1}^n \left(\frac{(n-1)!}{(k-1)!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!} \right) = (n-1)!, \quad (10)$$

а відповідна ймовірність появи такої фіксованої точки (для заданого початкового значення $y_i \in Y$) у випадково обраній підстановці степеня n матиме вигляд:

$$\sum_{k=1}^n P(\chi_{n,L=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = \frac{(n-1)!}{n!} = \frac{1}{n}. \quad (11)$$

Пояснимо формулу (9). Всього існують точно C_n^k способів одночасного обрання значень $y_i, y_{j_1}, y_{j_2}, \dots, y_{j_{k-1}} \in Y$, $y_i \neq y_{j_1} \neq y_{j_2} \neq \dots \neq y_{j_{k-1}}$, які однозначно визначають цикли $(y_i)(y_{j_1})(y_{j_2}) \dots (y_{j_{k-1}})$ довжиною $L = 1$. Але для кожного фіксованого $y_i \in Y$ існує точно C_{n-1}^{k-1} варіантів обрання решти значень $y_{j_1}, y_{j_2}, \dots, y_{j_{k-1}} \in Y$. Тобто із загальної кількості $n!P(\chi_{n,L=1} = k)$ тих підстановок, які містять k циклів довжини $L = 1$, тільки

$$n!P(\chi_{n,L=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = n!P(\chi_{n,L=1} = k) \frac{k}{n}$$

підстановок обов'язково міститимуть цикл (y_i) .

Остання формула (11) може бути отримана значно простіше з тривіальних комбінаторних міркувань. Дійсно, якщо на множині $Y = \{y_1, y_2, \dots, y_n\}$ зафіксувати m елементів, тоді можливі $(n-m)!$ варіантів перестановок решти елементів. Тобто на всій множині підстановок з S_n при їх випадковому рівномірному розподілі ймовірність обрати підстановку з m фіксованими точками дорівнює

$$\frac{(n-m)!}{n!} = \frac{1}{(n-m+1)(n-m+2) \dots n} = \frac{1}{(n)_m}, \quad (12)$$

що при $m=1$ співпадає з (11).

Формули (9–12) були отримані у роботі [10], в ході дослідження режиму вибіркового гамування із прискореним виробленням імітовставки (Galois/Counter Mode and GMAC – GCM & GMAC), що дозволило оцінити ймовірність виникнення нульового субключа гешування, тобто ймовірність такої події, коли при шифруванні нульового відкритого тексту буде отримано нульове значення шифртексту. Поширимо отриманий раніше результат на довільне значення до-

вжини циклу $L = l_i \in \{1, 2, \dots, n\}$ в ході дослідження періодичних властивостей гами у режимі OFB.

Розглянемо випадок довільної довжини циклу, тобто підрахуємо кількість таких підстановок s із S_n , які для довільного фіксованого $y_i \in Y$ обов'язково матимуть цикл

$$(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i))$$

довжини $L = l_i \in \{1, 2, \dots, n\}$.

Для фіксованих довжин та кількостей циклів $(L \text{ і } k)$ всього існує точно C_n^{kL} способів одночасного обрання значень

$$\begin{aligned} & y_i, y_{j_1}, y_{u_1}, \dots, y_{v_1}, \\ & y_{i_1}, y_{j_1}, y_{u_1}, \dots, y_{v_1}, \\ & y_{i_2}, y_{j_2}, y_{u_2}, \dots, y_{v_2}, \\ & \dots, \\ & y_{i_{k-1}}, y_{j_{k-1}}, y_{u_{k-1}}, \dots, y_{v_{k-1}}, \end{aligned} \quad (13)$$

які в сукупності визначають k циклів довжини L кожний:

$$\begin{aligned} & (y_i, y_j = s_i(y_i), y_u = s_i^2(y_i), \dots, y_v = s_i^{L-1}(y_i)), \\ & (y_{i_1}, y_{j_1} = s_{i_1}(y_{i_1}), y_{u_1} = s_{i_1}^2(y_{i_1}), \dots, y_{v_1} = s_{i_1}^{L-1}(y_{i_1})), \\ & (y_{i_2}, y_{j_2} = s_{i_2}(y_{i_2}), y_{u_2} = s_{i_2}^2(y_{i_2}), \dots, y_{v_2} = s_{i_2}^{L-1}(y_{i_2})), \\ & \dots, \\ & (y_{i_{k-1}}, y_{j_{k-1}} = s_{i_{k-1}}(y_{i_{k-1}}), y_{u_{k-1}} = s_{i_{k-1}}^2(y_{i_{k-1}}), \dots, y_{v_{k-1}} = s_{i_{k-1}}^{L-1}(y_{i_{k-1}})), \end{aligned} \quad (14)$$

причому всі елементи із (13) є унікальними (неповторними), адже сукупність циклів (14) входить до розкладу однієї і тієї ж підстановки.

Із C_n^{kL} способів одночасного обрання значень (13) для кожного фіксованого набору $y_i, y_{j_1}, y_{u_1}, \dots, y_{v_1} \in Y$ існує точно C_{n-1}^{kL-1} варіантів обрання решти значень

$$\begin{aligned} & y_{i_1}, y_{j_1}, y_{u_1}, \dots, y_{v_1}, \\ & y_{i_2}, y_{j_2}, y_{u_2}, \dots, y_{v_2}, \\ & \dots, \\ & y_{i_{k-1}}, y_{j_{k-1}}, y_{u_{k-1}}, \dots, y_{v_{k-1}}, \end{aligned}$$

бо обрання набору $y_i, y_{j_1}, y_{u_1}, \dots, y_{v_1} \in Y$ визначається через обрання тільки одного елементу $y_i \in Y$, а з решти $n-1$ елементів можливі різні комбінації по $kL-1$ елементів.

Таким чином, для кожного $k = 0, 1, \dots, [n/L]$ із загальної кількості $n!P(\chi_{n,L} = k)$ тих підстановок, які містять k циклів довжини L , тільки

$$\begin{aligned} n!P(\chi_{n,L} = k) \frac{C_{n-1}^{kL-1}}{C_n^{kL}} &= n!P(\chi_{n,L} = k) \frac{(n-1)!kL!(n-kL)!}{n!(kL-1)!(n-kL)!} = \\ &= n!P(\chi_{n,L} = k) \frac{kL}{n} = (n-1)!kLP(\chi_{n,L} = k) \end{aligned}$$

підстановок обов'язково міститимуть цикл

$$(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i)).$$

⁶ Цей набір $y_i, y_{j_1}, y_{u_1}, \dots, y_{v_1} \in Y$ складає цикл $(y_i, y_j = s_i(y_i), y_u = s_i^2(y_i), \dots, y_v = s_i^{L-1}(y_i))$, ймовірність появи якого у випадково обраній підстановці і треба визначити

Підсумувавши останній вираз за всіма $k = 0, 1, \dots, [n/L]$ із урахуванням (7), отримаємо точну формулу для визначення кількості підстановок s із S_n , які для довільного фіксованого $y_i \in Y$ обов'язково матимуть цикл

$$(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i))$$

довжини $L = l_i \in \{1, 2, \dots, n\}$:

$$\sum_{k=1}^{[n/L]} n! P(\chi_{n,L} = k) \frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \sum_{k=1}^{[n/L]} \frac{(n-1)!}{(k-1)! L^{k-1}} \sum_{j=0}^{[n/L]-k} \frac{(-1)^j}{L^j j!} = (n-1)!, \quad (15)$$

та відповідну формулу для розрахунку ймовірності випадково обрати підстановку s із S_n з таким циклом:

$$\sum_{k=1}^{[n/L]} P(\chi_{n,L} = k) \frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \frac{(n-1)!}{n!} = \frac{1}{n}. \quad (16)$$

Очевидно, що останній аналітичний вираз при $L=1$ повністю збігається з формулою (8) у [10] з відповідним викладенням.

Отриманий аналітичний вираз (16) може розглядатися і як комбінаторна тотожність (спрощена формула) для суми членів формули (7) із відповідними пропорційними коефіцієнтами

$$\frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \frac{kL}{n},$$

або навіть для розподілу Пуассона (8).

Оцінку ймовірності (16) виникнення циклу певної довжини можна, як і в роботі [10], отримати іншим, значно простішим способом, застосовуючи прості комбінаторні міркування.

Зафіксуємо деяке довільне значення y_i із множини $Y = \{y_1, y_2, \dots, y_n\}$. Всього існує $n!$ підстановок на множині Y , з яких лише

$$\frac{n!}{n} = (n-1)!$$

підстановок міститимуть цикл (y_i) довжини $L=1$ у своєму цикловому розкладі.

Крім того, із $n!$ підстановок симетричної групи

$$\frac{n!}{n(n-1)}(n-1) = (n-1)!$$

підстановок міститимуть цикл $(y_i, y_{j \neq i})$ довжини $L=2$,

$$\frac{n!}{n(n-1)(n-2)}(n-1)(n-2) = (n-1)!$$

підстановок міститимуть цикл $(y_i, y_{j \neq i}, y_{u \neq i,j})$ довжини $L=3$ і т.д.

Тобто для довільного фіксованого значення $y_i \in Y$ кількість підстановок із S_n , які містять цикл $(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i))$, визначається як $(n-1)!$, а відповідна ймовірність випадково обрати підстановку, що містить такий цикл, визначається як

$$\frac{(n-1)!}{n!} = \frac{1}{n},$$

незалежно ані від довжини циклу $L = l_i \in \{1, 2, \dots, n\}$, ані від власного значення y_i із $Y = \{y_1, y_2, \dots, y_n\}$.

Таким чином, ймовірність виникнення циклу певної довжини визначається лише за степенем підстановки n . Наприклад, для $n=4$ із $n! = 24$ підстановок симетричної групи для будь-якого фіксованого y_i із $Y = \{y_1, y_2, y_3, y_4\}$ маємо по $(n-1)! = 6$ підстановок, які обов'язково містять цикли різної довжини (або (y_i) , або $(y_i, y_{j \neq i})$, або $(y_i, y_{j \neq i}, y_{u \neq i,j})$, або $(y_i, y_{j \neq i}, y_{u \neq i,j}, y_{v \neq i,j,u})$, відповідно). Отже ймовірність того, що у випадково обраній підстановці із S_4 міститиметься цикл довжини $L = l_i \in \{1, 2, \dots, 4\}$, дорівнюватиме $1/n = 1/4$ незалежно ані від y_i , ані від $L = l_i$.

Оскільки отримані аналітичні вирази (15) та (16) досить складні та громіздкі, особливо порядок їхнього виведення, проілюструємо приклад розрахунку ймовірностей появи циклу заданої довжини у випадково обраній підстановці із симетричної групи S_4 . Приклад доповнюватимемо поясненнями, що демонструють справедливості отриманих формул та наведених комбінаторних міркувань.

5. ПРИКЛАД ДЛЯ СИМЕТРИЧНОЇ ГРУПИ S_4

Розглянемо приклад усіх бієктивних перетворень множини $Y = \{y_1, y_2, y_3, y_4\}$ саму в себе, тобто множину із $n! = 24$ підстановок степеня $n = 4$.

У таблиці 1 наведено всі підстановки, які складають симетричну групу S_4 (наведено результати кожної підстановки, розклад кожної підстановки на цикли, загальна кількість циклів та розподіл кількості циклів певної довжини. Кожну підстановку для зручності пронумеровано).

У таблиці 2 наведено розподіли кількості величин $\xi_n = k$ та $\chi_{n,L} = k$ для різних k (символом # (x) позначено число випадків (x) за всіма підстановками із S_4).

5.1 Оцінка ймовірності появи циклу (y_i) . Розглянемо випадок, коли для довільного фіксованого $y_i \in Y$ випадково обрана підстанова s із S_4 обов'язково міститиме цикл (y_i) довжини $L=1$.

Спочатку розглянемо ті підстановки, які містять $k=1$ цикл довжини $L=1$. Маємо 8 таких підстановок (табл. 3)⁷. Але кожне окреме $y_i \in Y$ породжує цикл довжини $L=1$ лише двічі, тобто для кожного довільного фіксованого $y_i \in Y$ існує точно 2 підстановки, які містять цикл довжини $L=1$ виду (y_i) . Наприклад, для $y_1 \in Y$ це 4-та та 5-та підстановки, для $y_2 \in Y$ це 16-та та 21-ша підстанова і т.д. Кількість підстановок, які для довільного фіксованого $y_i \in Y$ містять $k=1$, цикл довжини $L=1$ виду (y_i) підрахуємо наступним чином. Всього існує точно $C_{n=4}^{kL=1} = 4$ способів обрання значення $y_i \in Y$.

⁷ Номера підстановок у таблицях 3–5 відповідають загальній нумерації підстановок із таблиці 1

Множина підстановок із S_4 та їх циклові властивості

№ з/п	Результат підстановки				Розклад підстановки на цикли	Число циклів, ξ_n	Число циклів довжини L , $\chi_{n,L}$			
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$			$L = 1$	$L = 2$	$L = 3$	$L = 4$
1	y_1	y_2	y_3	y_4	$(y_1) (y_2) (y_3) (y_4)$	4	4	0	0	0
2	y_1	y_2	y_4	y_3	$(y_1) (y_2) (y_3, y_4)$	3	2	1	0	0
3	y_1	y_3	y_2	y_4	$(y_1) (y_2, y_3) (y_4)$	3	2	1	0	0
4	y_1	y_3	y_4	y_2	$(y_1) (y_2, y_3, y_4)$	2	1	0	1	0
5	y_1	y_4	y_2	y_3	$(y_1) (y_2, y_4, y_3)$	2	1	0	1	0
6	y_1	y_4	y_3	y_2	$(y_1) (y_2, y_4) (y_3)$	3	2	1	0	0
7	y_2	y_1	y_3	y_4	$(y_1, y_2) (y_3) (y_4)$	3	2	1	0	0
8	y_2	y_1	y_4	y_3	$(y_1, y_2) (y_3, y_4)$	2	0	2	0	0
9	y_2	y_3	y_1	y_4	$(y_1, y_2, y_3) (y_4)$	2	1	0	1	0
10	y_2	y_3	y_4	y_1	(y_1, y_2, y_3, y_4)	1	0	0	0	1
11	y_2	y_4	y_1	y_3	(y_1, y_2, y_4, y_3)	1	0	0	0	1
12	y_2	y_4	y_3	y_1	$(y_1, y_2, y_4) (y_3)$	2	1	0	1	0
13	y_3	y_1	y_2	y_4	$(y_1, y_3, y_2) (y_4)$	2	1	0	1	0
14	y_3	y_1	y_4	y_2	(y_1, y_3, y_4, y_2)	1	0	0	0	1
15	y_3	y_2	y_1	y_4	$(y_1, y_3) (y_2) (y_4)$	3	2	1	0	0
16	y_3	y_2	y_4	y_1	$(y_1, y_3, y_4) (y_2)$	2	1	0	1	0
17	y_3	y_4	y_1	y_2	$(y_1, y_3) (y_2, y_4)$	2	0	2	0	0
18	y_3	y_4	y_2	y_1	(y_1, y_3, y_2, y_4)	1	0	0	0	1
19	y_4	y_1	y_2	y_3	(y_1, y_4, y_3, y_2)	1	0	0	0	1
20	y_4	y_1	y_3	y_2	$(y_1, y_4, y_2) (y_3)$	2	1	0	1	0
21	y_4	y_2	y_1	y_3	$(y_1, y_4, y_3) (y_2)$	2	1	0	1	0
22	y_4	y_2	y_3	y_1	$(y_1, y_4) (y_2) (y_3)$	3	2	1	0	0
23	y_4	y_3	y_1	y_2	(y_1, y_4, y_2, y_3)	1	0	0	0	1
24	y_4	y_3	y_2	y_1	$(y_1, y_4) (y_2, y_3)$	2	0	2	0	0

Таблиця 2

Розподіли кількості величин $\xi_n = k$ та $\chi_{n,L} = k$
за всіма підстановками із S_4

k	0	1	2	3	4
$\# (\xi_n = k)$	0	6	11	6	1
$\# (\chi_{n,L=1} = k)$	9	8	6	0	1
$\# (\chi_{n,L=2} = k)$	15	6	3	0	0
$\# (\chi_{n,L=3} = k)$	16	8	0	0	0
$\# (\chi_{n,L=4} = k)$	18	6	0	0	0

Таблиця 3

Підстановки, що містять 1 цикл довжини 1
та один цикл довжини 3

№ з/п	Результат підстановки				Розклад підстановки на цикли
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
4	y_1	y_3	y_4	y_2	$(y_1) (y_2, y_3, y_4)$
5	y_1	y_4	y_2	y_3	$(y_1) (y_2, y_4, y_3)$
9	y_2	y_3	y_1	y_4	$(y_1, y_2, y_3) (y_4)$
12	y_2	y_4	y_3	y_1	$(y_1, y_2, y_4) (y_3)$
13	y_3	y_1	y_2	y_4	$(y_1, y_3, y_2) (y_4)$
16	y_3	y_2	y_4	y_1	$(y_1, y_3, y_4) (y_2)$
20	y_4	y_1	y_3	y_2	$(y_1, y_4, y_2) (y_3)$
21	y_4	y_2	y_1	y_3	$(y_1, y_4, y_3) (y_2)$

Цей вибір більш нічим не обмежується, бо для кожного $y_i \in Y$ цикл (y_i) визначається однозначно (за формулою існує $C_{n-1=3}^{kL-1=0} = 1$ варіантів

обрання значення $y_{j \neq i} \in Y$). Тобто загальну кількість підстановок, які містять тільки $k = 1$, цикл довжини $L = 1$ (таких вісім підстановок) треба

помножити на величину $\frac{C_{n-1=3}^{kL-1=0}}{C_{n=4}^{kL=1}} = \frac{1}{4}$. Таким чи-

ном, для довільного фіксованого $y_i \in Y$ число підстановок, які містять тільки один цикл (y_i) , дорівнює двом.

Таблиця 4

Підстановки, що містять два цикли довжини 1
та один цикл довжини 2

№ з/п	Результат підстановки				Розклад підстановки на цикли
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
2	y_1	y_2	y_4	y_3	$(y_1) (y_2) (y_3, y_4)$
3	y_1	y_3	y_2	y_4	$(y_1) (y_2, y_3) (y_4)$
6	y_1	y_4	y_3	y_2	$(y_1) (y_2, y_4) (y_3)$
7	y_2	y_1	y_3	y_4	$(y_1, y_2) (y_3) (y_4)$
15	y_3	y_2	y_1	y_4	$(y_1, y_3) (y_2) (y_4)$
22	y_4	y_2	y_3	y_1	$(y_1, y_4) (y_2) (y_3)$

Розглянемо тепер ті підстановки, які містять по $k = 2$ цикли довжини $L = 1$. Маємо 6 підстановок (табл. 4), із них три підстановки у цикловому розкладі містять цикли $(y_1) (y_{i \neq 1})$, три підстановки містять цикли $(y_2) (y_{i \neq 2})$, три підстановки містять цикли $(y_3) (y_{i \neq 3})$ і три підстановки містять цикли $(y_4) (y_{i \neq 4})$. Зрозуміло, що одна і та ж підстановка може рахуватися по-різному, тобто

може за своїм цикловим розкладом відноситися як до підстановок, що містять цикли $(y_i) (y_{j \neq i})$, так і до підстановок, що містять цикли $(y_j) (y_{i \neq j})$. Наприклад, шоста підстановка має цикловий розклад $(y_1) (y_2, y_4) (y_3)$, вона має рахуватися як із підстановками із циклами $(y_1) (y_{j \neq 1})$, так і з підстановками із циклами $(y_3) (y_{i \neq 3}) (y_{j \neq 3})$.

Кількість підстановок, які для фіксованого $y_i \in Y$ містять $k = 2$ цикли $(y_i) (y_{j \neq i})$ довжини $L = 1$, підрахуємо наступним чином. Всього існує точно $C_{n=4}^{kL=2} = 6$ способів одночасного обрання значень $y_i, y_{j \neq i} \in Y$. Але для фіксованого $y_i \in Y$ наявні точно $C_{n=3}^{kL-1=1} = 3$ варіанти обрання значення $y_{j \neq i} \in Y$. Тобто загальну кількість підстановок, які містять $k = 2$ цикли довжини $L = 1$, треба

помножити на величину $\frac{C_{n=3}^{kL-1=1}}{C_{n=4}^{kL=2}} = \frac{3}{6}$, отримаємо

шукане значення — для довільного фіксованого значення $y_i \in Y$ число підстановок, містять $k = 2$ цикли $(y_i) (y_{j \neq i})$ довжини $L = 1$, дорівнює трьом. Наприклад, для фіксованого значення $y_1 \in Y$ друга, третя та шоста підстановки містять по $k = 2$ цикли довжини $L = 1$ із цикловими розкладами: $(y_1) (y_2) (y_3, y_4)$, $(y_1) (y_2, y_3) (y_4)$ та $(y_1) (y_2, y_4) (y_3)$.

Розглянемо підстановки, які містять $k = 4$ цикли довжини $L = 1$ ($k = 3$ цикли довжини $L = 1$ жодна підстановка мати не може). Маємо одну підстановку — ту, яка наведена першою у табл. 1, її цикловий розклад має вигляд: $(y_1) (y_2) (y_3) (y_4)$. Застосувавши ту ж саму формулу, маємо $\frac{C_{n=3}^{kL-1=3}}{C_{n=4}^{kL=4}} = \frac{1}{1} = 1$, тобто загальна кількість підстановок, які містять чотири цикли довжини 1 співпадає із кількістю підстановок із цикловим розкладом $(y_i) (y_{j \neq i}) (y_{u \neq i,j}) (y_{v \neq i,j,u})$, як це і має бути.

Підрахуємо кількість підстановок із S_4 (табл. 1), які для фіксованого $y_i \in Y$ обов'язково містять цикл (y_i) довжини $L = 1$. Для цього треба підсумувати кількість підстановок, які для фіксованого $y_i \in Y$ у своєму цикловому розкладі містять різну кількість циклів довжини $L = 1$, а саме, це 2 підстановки із $k = 1$ циклом (y_i) , три підстановки із $k = 2$ циклами $(y_i) (y_{j \neq i})$ та одна підстановка із $k = 4$ циклами $(y_i) (y_{j \neq i}) (y_{u \neq i,j}) (y_{v \neq i,j,u})$. Загалом маємо 6 підстановок із загальної кількості 24 підстановок симетричної групи. Тобто при випадковому рівномірному обранні підстановки із S_4 ймовірність того, що в ній для довільного фіксованого $y_i \in Y$ спостерігатиметься цикл (y_i) довжини $L = 1$ дорівнює $6/24 = 1/4$.

5.2. Оцінка ймовірності появи циклу $(y_i, y_{j \neq i})$. Розглянемо випадок, коли для довільного фіксованого $y_i \in Y$ випадково обрана підстановка s із S_4 обов'язково міститиме цикл $(y_i, y_{j \neq i})$ довжини $L = 2$.

Спочатку розглянемо ті підстановки, які містять $k = 1$ цикл довжини $L = 2$. Маємо 6 таких підстановок, які наведено у таблиці 4 (якщо підстановка із S_4 містить два цикли довжини 1, тоді вона обов'язково містить один цикл до-

вжини 2). Підрахуємо кількість підстановок, які для довільного фіксованого $y_i \in Y$ містять $k = 1$ цикл довжини $L = 2$ виду $(y_i, y_{j \neq i})$. Всього є точно $C_{n=4}^{kL=2} = 6$ способів одночасного обрання значень $y_i, y_{j \neq i} \in Y$. Але для кожного $y_i \in Y$ існує точно $C_{n=3}^{kL-1=1} = 3$ варіанта обрання значення $y_{j \neq i} \in Y$. Тобто число підстановок, які для довільного фіксованого $y_i \in Y$ у цикловому розкладі містять $k = 2$ цикли $(y_i) (y_{j \neq i})$ довжини $L = 1$, дорівнює $6 \cdot \frac{C_{n=3}^{kL-1=1}}{C_{n=4}^{kL=2}} = 3$. Наприклад, для $y_1 \in Y$ сьома, п'ятнадцята та двадцять друга підстановки містять по $k = 1$ цикли довжини $L = 2$.

Розглянемо також ті підстановки, які містять по $k = 2$ цикли довжини $L = 2$. Всього в S_n є 3 таких підстановки, це (див. табл. 1):

- восьма підстановка із цикловим розкладом $(y_1, y_2) (y_3, y_4)$;
- сімнадцята підстановка із цикловим розкладом $(y_1, y_3) (y_2, y_4)$;
- остання, двадцять четверта підстановка із цикловим розкладом $(y_1, y_4) (y_2, y_3)$.

Кількість підстановок, які для довільного фіксованого $y_i \in Y$ містять $k = 2$ цикли $(y_i, y_{j \neq i})$ та $(y_{u \neq i,j}, y_{v \neq i,j,u})$ довжини $L = 2$, підраховується так само. Всього існує точно $C_{n=4}^{kL=4} = 1$ способів одночасного обрання значень $y_i, y_{j \neq i}, y_{u \neq i,j}, y_{v \neq i,j,u} \in Y$. Цей вибір більш нічим не обмежується, бо для обраних $y_i, y_{j \neq i}, y_{u \neq i,j}, y_{v \neq i,j,u} \in Y$ відповідні $k = 2$ цикли $(y_i, y_{j \neq i})$ та $(y_{u \neq i,j}, y_{v \neq i,j,u})$ визначаються однозначно (за формулою існує $C_{n=3}^{kL-1=3} = 1$ варіантів). Тобто, число підстановок, які для довільного фіксованого значення $y_i \in Y$ мають цикловий розклад $(y_i, y_{j \neq i}) (y_{u \neq i,j}, y_{v \neq i,j,u})$, збігається із загальним числом підстановок із $k = 2$ циклами довжини $L = 2$, тобто дорівнює 3.

Оскільки $k = 3$ та $k = 4$ цикли довжини $L = 2$ жодна підстановка із S_4 мати не може, одразу перейдемо до підрахунку ймовірності виникнення циклу $(y_i, y_{j \neq i})$ у випадково обраній підстановці. Для цього підсумуємо кількість підстановок, які для довільного фіксованого $y_i \in Y$ у своєму цикловому розкладі містять різну кількість циклів довжини $L = 2$, а саме, це 3 підстановки із $k = 1$ циклом $(y_i, y_{j \neq i})$, та три підстановки із $k = 2$ циклами $(y_i, y_{j \neq i}) (y_{u \neq i,j}, y_{v \neq i,j,u})$. Загалом маємо 6 підстановок із загальної кількості 24 підстановок симетричної групи, тобто при випадковому обранні підстановки із S_4 ймовірність того, що в ній для довільного фіксованого $y_i \in Y$ спостерігатиметься цикл $(y_i, y_{j \neq i})$ довжини $L = 2$ дорівнює $6/24 = 1/4$.

5.3. Оцінка ймовірності появи циклу $(y_i, y_{j \neq i}, y_{u \neq i,j})$. Аналогічно до розглянутого вище, підрахуємо кількість підстановок, які для довільного фіксованого $y_i \in Y$ мають цикл $(y_i, y_{j \neq i}, y_{u \neq i,j})$. У довільній підстановці $s \in S_4$ може бути не більше одного такого циклу, тобто випадки із $k > 1$ неможливі. Кожен цикл довжини $L = 3$ у розкладанні підстановки поєднується із циклом

довжини 1, тобто всі 8 таких підстановок наведено табл. 3.

Підрахуємо кількість тих підстановок, які для довільного фіксованого $y_i \in Y$ обов'язково містять цикл $(y_i, y_{j \neq i}, y_{u \neq i, j})$. Всього наявні точно $C_{n=4}^{kL=3} = 4$ способи одночасного обрання значень $y_i, y_{j \neq i}, y_{u \neq i, j} \in Y$. Але для кожного $y_i \in Y$ існує точно $C_{n=3}^{kL-1=2} = 3$ варіанта обрання значень $y_{j \neq i}, y_{u \neq i, j} \in Y$. Тобто число підстановок, які для довільного фіксованого значення $y_i \in Y$ обов'язково мають цикл $(y_i, y_{j \neq i}, y_{u \neq i, j})$, визначається як $8 \cdot \frac{C_{n=3}^{kL-1=2}}{C_{n=4}^{kL=3}} = 6$. Наприклад, для $y_1 \in Y$ це 6

підстановок (№ 9, 12, 13, 16, 20, 21) із цикловими розкладами (див. табл. 3): $(y_1, y_2, y_3) (y_4)$, $(y_1, y_2, y_4) (y_3)$, $(y_1, y_3, y_2) (y_4)$, $(y_1, y_3, y_4) (y_2)$, $(y_1, y_4, y_2) (y_3)$ та $(y_1, y_4, y_3) (y_2)$.

Отже, ймовірність того, що для довільного фіксованого $y_i \in Y$ у випадково обраній підстановці $s \in S_4$ спостерігатиметься цикл $(y_i, y_{j \neq i}, y_{u \neq i, j})$ довжини $L = 3$ дорівнює $6/24 = 1/4$.

5.4. Оцінка ймовірності появи циклу $(y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u})$. У будь-якій підстановці $s \in S_4$ може бути тільки один цикл довжини $L = 4$. Такі підстановки наведено у таблиці 5.

Таблиця 5

Підстановки, що містять один цикл довжини 4

№ з/п	Результат підстановки				Розклад підстановки на цикли
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
10	y_2	y_3	y_4	y_1	(y_1, y_2, y_3, y_4)
11	y_2	y_4	y_1	y_3	(y_1, y_2, y_4, y_3)
14	y_3	y_1	y_4	y_2	(y_1, y_3, y_4, y_2)
18	y_3	y_4	y_2	y_1	(y_1, y_3, y_2, y_4)
19	y_4	y_1	y_2	y_3	(y_1, y_4, y_3, y_2)
23	y_4	y_3	y_1	y_2	(y_1, y_4, y_2, y_3)

Очевидно, що всі такі підстановки обов'язково мають у своєму єдиному циклі всі елементи із множини $Y = \{y_1, y_2, y_3, y_4\}$, тобто, для кожного $y_i \in Y$ у кожній підстановці із табл. 5 існуватиме цикл $(y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u})$. Перевіримо застосовану вище формулу: $\frac{C_{n=4}^{kL-1=3}}{C_{n=4}^{kL=4}} = 1$, тобто дійсно, всі підстановки із таблиці 5 обов'язково міститимуть цикл $(y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u})$ для кожного довільного фіксованого $y_i \in Y$.

Отже, ймовірність появи циклу $(y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u})$ у випадково обраній підстановці $s \in S_4$ дорівнює $6/24 = 1/4$.

6. ІНТЕРПРЕТАЦІЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ ДО ВЛАСТИВОСТЕЙ БСШ

Отримані аналітичні вирази (15) та (16) дозволяють оцінити кількість підстановок із симетричної групи, які для визначеного елемента множини перетворень обов'язково містять цикл певної довжини із цим елементом, та відповідну ймовірність випадково обраної підстановки із таким циклом.

Скористаємося цими формулами для дослідження періодичних властивостей гами у режимі OFB. При цьому вважатимемо, що ймовірнісні властивості підстановок, які утворюються шифрувальною функцією, відповідають певним властивостям випадкової підстановки, тобто відповідають нашим уявленням про такий «ідеальний» БСШ, який при будь-якому введеному ключі шифрування випадково і рівномірно зіставляє будь-який шифртекст будь-якому відкритому тексту. Таким чином l -бітний БСШ реалізовуватиме деяку підмножину симетричної групи підстановок степеня 2^l , обрання конкретної підстановки s із S_{2^l} пов'язується із введеним ключем шифрування. На всій множині ключів шифру ймовірність обрати таку підстановку, яка для довільного фіксованого $y_i = S \in Y = \{y_1, y_2, \dots, y_{2^l}\}$ обов'язково має цикл $(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i))$ довжини $L = l_i \in \{1, 2, \dots, n\}$, визначатиметься за (16).

Практично це означає, що ймовірність виникнення циклу будь-якої довжини у випадково вибраній підстановці з симетричної групи S_{2^l} для довільного фіксованого елемента множини не залежить ні від цього елемента, ні від довжини циклу. Вона залежить лише від порядку $n = 2^l$ підстановок симетричної групи S_n і визначається як зворотна величина, тобто дорівнює $1/n$. Для будь-якого фіксованого значення введеної синхропосилки $y = S$ ймовірність того, що відповідна шифрграма $\gamma_i, i = 0, 1, \dots, n-1$, яка формується у режимі OFB, матиме період довжини $L = l_i \in \{1, 2, \dots, n\}$, не залежить ані від значення цієї синхропосилки, ані від довжини періоду. Вона визначається лише степенем підстановки, тобто, у даному випадку, розрядністю шифру і дорівнює 2^{-l} .

Визначимо ймовірність того, що період формованої шифрграми буде не меншим за 2^m блоків, тобто ймовірність такої події, коли для фіксованого значення введеної синхропосилки $y_i = S$ відповідна шифрграма не повторюватиметься під час виконання 2^m ітерацій за формулами (1), (3) при формуванні блоків гами γ_i :

$$P(\forall i, j \in \{1, 2, \dots, 2^m\} : \gamma_i \neq \gamma_j | i \neq j) = 1 - \sum_{L=1}^{2^m} \sum_{k=1}^{[2^l/L]} P(\chi_{2^l, L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}} = \sum_{L=2^m+1}^{2^l} \sum_{k=1}^{[2^l/L]} P(\chi_{2^l, L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}}. \quad (17)$$

Враховуючи (16), отримаємо:

$$P(\forall i, j \in \{1, 2, \dots, 2^m\} : \gamma_i \neq \gamma_j | i \neq j) = 1 - \sum_{L=1}^{2^m} 2^{-l} = \sum_{L=2^m+1}^{2^l} 2^{-l} = 1 - 2^{m-l}. \quad (18)$$

Таким чином, в ході виконання припущення щодо відповідності певних ймовірнісних власти-

востей шифру властивостям випадкової підстановки ймовірність неповторення ґами на визначеній довжині є функцією від цієї довжини. Цей факт зумовлює основні обмеження на застосування режиму ґамування зі зворотним зв'язком за шифрґамою, що безпосередньо впливає із отриманих результатів досліджень. Так, що стосується відповідного режиму застосування БСШ «Калина», специфікацію якого наведено у [1, 2], основним обмеженням на використання режиму OFB є вказані в додатку Г.2 «Обмеження на сумарну довжину повідомлень, що захищаються з використанням одного ключа», а саме:

- при розмірі блоку 128 біт рекомендується обмежити кількість блоків, що захищаються на одному ключі величиною 2^{60} (16 млн ТБ);
- при розмірі блоку 256 біт рекомендується обмежити кількість блоків, що захищаються на одному ключі величиною 2^{124} ;
- при розмірі блоку 512 біт рекомендується обмежити кількість блоків, що захищаються на одному ключі величиною 2^{251} .

Оскільки, як це показано у розділі 2, сутність захисту інформаційного повідомлення за специфікацією режиму OFB полягає у додаванні до нього шифрґами, тоді обмеження, вказані у додатку Г.2 стосуються саме обмежень на довжину шифрґами, яка формується багаторазовим шифруванням одного і того ж несекретного блоку ініціалізації (синхроросилки) за формулами (1), (3). Тобто, виконання обмежень, які рекомендовано специфікацією проекту національного стандарту, забезпечує певні ймовірнісні показники неперіодичності шифрґами, а саме:

- при розмірі блоку $l = 128$ біт і при виконанні рекомендованого обмеження кількості блоків, що захищаються на одному ключі величиною $2^m = 2^{60}$, буде забезпечено ймовірність неповторення ґами $1 - 2^{m-l} = 1 - 2^{-68} > 1 - 2^{-64}$;
- при розмірі блоку $l = 256$ біт і при виконанні рекомендованого обмеження кількості блоків, що захищаються на одному ключі величиною $2^m = 2^{124}$, буде забезпечено ймовірність неповторення ґами $1 - 2^{m-l} = 1 - 2^{-132} > 1 - 2^{-128}$;
- при розмірі блоку $l = 512$ біт і при виконанні рекомендованого обмеження кількості блоків, що захищаються на одному ключі величиною $2^m = 2^{251}$, буде забезпечено ймовірність неповторення ґами $1 - 2^{m-l} = 1 - 2^{-261} > 1 - 2^{-256}$.

Частіше в теорії захисту інформації застосовують зворотну величину – ймовірність того, що сформована шифрґама із довжиною, що не перевищує певну межу, матиме хоча б одне повторення. Враховуючи (17) та (18) цю ймовірність визначимо як:

$$P_{l,m} = 1 - P(\forall i, j \in \{1, 2, \dots, 2^m\} : \gamma_i \neq \gamma_j |_{i \neq j}) = \sum_{L=1}^{2^m} \sum_{k=1}^{\lfloor 2^l / L \rfloor} P(\chi_{2^l, L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}} = 2^{m-l}. \quad (19)$$

На рис. 2 зображено залежність $P_{l,m}$ від m для різних l .

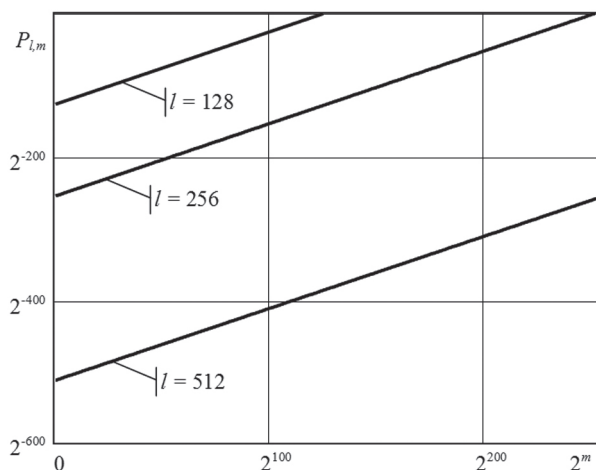


Рис. 2. Залежності ймовірності того, що у шифрґамах $\gamma_i, i = 0, 1, \dots, n-1$ довжиною не більше $2^m = 2^{60}$ блоків буде хоча б одне повторення

Із залежностей, які наведено на рис. 2, видно, що підвищення довжини шифрґами веде до зростання ймовірності будь-якої кількості повторень блоків ґами. Ці графіки можна застосовувати для обґрунтування певних обмежень, наприклад, якщо потрібно зменшити ймовірність будь-якої кількості повторень ґами необхідно зменшити її довжину.

ВИСНОВКИ

На підставі отриманих результатів можна зробити такі важливі у практичному значенні висновки.

1. Властивості сучасних симетричних криптоперетворень залежать не лише від характеристик БСШ, але й від режимів його застосування. Тому у проекті національного стандарту ДСТУ «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» передбачено 10 режимів криптоперетворення: проста заміна (базове перетворення), ґамування, ґамування зі зворотним зв'язком за шифртекстом, вироблення імітовставки, зчеплення шифрблоків, ґамування зі зворотним зв'язком за шифрґамою, вибіркове ґамування із прискореним виробленням імітовставки, вироблення імітовставки і ґамування, індексованої заміни, захисту ключових даних.

2. У режимі OFB, який застосовується для забезпечення послуги конфіденційності, вихідне повідомлення захищається шляхом додавання шифрґами, яка формується багаторазовим шифруванням одного і того ж несекретного блоку ініціалізації (синхроросилки). Якщо прийняти припущення про відповідність властивостей шифру певним властивостям випадкової підстановки, тоді періодичність ґами визначатиметься наявністю циклів у випадково обраній підстановці із симетричної групи, причому обрання підстановки задається значенням секретного ключа.

3. Дослідження властивостей випадково обраної підстановки s з симетричної групи S_n показали, що ймовірність виникнення циклу $s_i = (y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{l_i-1}(y_i))$ будь-якої довжини $L = l_i$ для довільного фіксованого елементу y_i з множини $Y = \{y_1, y_2, \dots, y_n\}$ не залежить ані від цього елементу y_i , ані від довжини циклу $L = l_i$. Ця ймовірність залежить лише від порядку n підстановок симетричної групи S_n і визначається як зворотна величина, тобто дорівнює $1/n$.

4. Таким чином, періодичні властивості гами у режимі гамування зі зворотним зв'язком за шифрною визначаються за розподілом ймовірностей кількості циклів випадкової підстановки. Обрання секретного ключа, який параметризує шифрувальну функцію, відповідає обранню конкретної підстановки із симетричної групи, обрання значення синхропосилки відповідає обранню елемента y_i з множини елементів $Y = \{y_1, y_2, \dots, y_n\}$, над якими здійснюється підстановка. Але ані власне значення синхропосилки, ані довжина періоду гами не впливають на ймовірність отримання гами певного періоду. Ця ймовірність визначається лише степенем підстановки $n = 2^l$, тобто за розрядністю l базового шифрувального перетворення.

5. З точки зору практичного застосування симетричних криптоперетворень до шифрними висуваються вимоги непереворотної на довжині, що не перевищує встановленої межі. Ймовірність такої події визначається як $1 - 2^{m-l}$, де 2^m — обмеження довжини шифрними. Наприклад, для 128-розрядного шифру «Калина» при обмеженні довжини гами до 2^m у режимі OFB ймовірність того, що блоки гами жодного разу не співпадають, дорівнює $1 - 2^{m-l} = 1 - 2^{-68}$, тобто значно більше за $1 - 2^{-64}$. Зворотна величина $P_{l,m}$, тобто ймовірність того, що на довжині не більше 2^m блоки шифрними в режимі OFB співпадають бодай один раз, дорівнюватиме $P_{l,m} = 2^{m-l}$. Ця залежність може використовуватися для обґрунтування обмежень на довжину шифрними, коли встановлена верхня межа ймовірності $P_{l,m}$.

6. Специфікацією БСШ «Калина» [1, 2] рекомендовано певні обмеження на сумарну довжину повідомлень, що захищаються з використанням одного ключа. Стосовно режиму гамування зі зворотним зв'язком за шифрною такі обмеження слід розглядати як вимоги до максимальної довжини гами, яка з певною ймовірністю не повторюватиметься. Наведені рекомендації носять принциповий характер, бо саме виникнення повторення гами є найбільш небезпечним випадком в ході застосування режиму OFB, адже в цьому разі зловмисник майже напевно порушить встановлений режим конфіденційності повідомлень. Наприклад, якщо допустима ймовірність повторення блоків гами складає 2^{-64} , тоді довжина гами для $l = 128$ бітного БСШ «Калина» не

має перевищувати 2^{64} блоків (у проекті стандарту це обмеження більш жорсткіше і складає 2^{60}).

7. Отримані оцінки ймовірності формування гами певного періоду можна розглядати і як критерій обрання криптографічних примітивів, або критерій статистичного тестування. Дійсно, якщо досліджуваний криптопримітив у режимі OFB з рівною ймовірністю формує гами будь-якого періоду і ця ймовірність визначається зворотною до степеня підстановки, тоді за циклічними властивостями досліджуваний криптопримітив відповідає ймовірнісним властивостям випадкової підстановки і за цим критерієм може бути прийнятий до застосування. Власне проведення таких досліджень, зокрема, на нелінійних вузлах заміни або на зменшених моделях БСШ є перспективним напрямком подальших робіт. Перспективним також є поширення отриманих результатів на інші режими гамування, зокрема, на режими гамування зі зворотним зв'язком за шифртекстом, вибіркового гамування із прискореним виробленням імітовставки, вироблення імітовставки і гамування тощо.

Література

- [1] ДСТУ. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. - Проект стандарту друга (остаточна) редакція. — Київ: Держспоживстандарт України, 2014. — 238 с.
- [2] Розробка нового блокового симетричного шифру: звіт за перший етап НДР «Алгоритм» (проміжний) / АТ «ІТ»; кер. І.Д. Горбенко — Харків, 2014. — Том 4. — 304 с.
- [3] Сачков В.Н. Введение в комбинаторные методы дискретной математики. — М.: Наука. Гл. ред. физ.-мат. лит., 1982. — 384 с.
- [4] Тронин С.Н. Введение в теорию групп. — Казань: Казанский государственный университет, 2006. — 100 с.
- [5] Александров П.С. Введение в теорию групп. — М.: Наука, — 1980. — 145 с.
- [6] Долгов В.И., Лисицкая И.В., Руженцев В.И. Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника — 2007. — Т. 6, № 2. — С. 257–263.
- [7] Кузнецов А.А., Лисицкая И.В., Исаев С.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс // Прикладная радиоэлектроника. — 2011. — Т. 10, №2 — С. 135–140.
- [8] Сорока Л.С., Кузнецов А.А., Московченко И.В., Исаев С.А. Исследование дифференциальных свойств блочно-симметричных шифров. // Системы обработки информации. — Х: ХУПС. — 2010 — Вип. 6(87). — С. 286–294.
- [9] Долгов В.И., Родинко М.Ю. Блочные симметричные шифры — случайные подстановки. Комбинаторные показатели // Прикладная радиоэлектроника — 2013. — Т.12, №2 — С. 236–239.
- [10] Кузнецов О. О. Анализ коллизийных властивостей режиму вироблення імітовставок із вибірко-

вим ґамуванням / О. О. Кузнецов, Д. В. Іваненко, Є.П. Колованова // Вісник Харківського національного університету ім. В. Н. Каразіна серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління». — 2014. — № 1097, Т. 23. — С. 55–71.

Надійшла до редколегії 2.09.2014

Кузнецов Олександр Олександрович, фото та відомості про автора див. на стор. 207.



Горбенко Юрій Іванович, кандидат технічних наук, технічний директор АТ “ІТ”. Наукові інтереси: криптографічні системи та протоколи, проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

Колованова Євгенія Павлівна, фото та відомості про автора див. на стор. 207.

УДК 004.056.55

Периодические свойства шифрґаммы в режиме Output Feedback / А.А. Кузнецов, Ю.И. Горбенко, Е.П. Колованова // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 239–251.

Исследуются свойства режима ґаммирования с обратной связью по шифрґамме (англоязычное обозначение — Output Feedback). С применением матема-

тического аппарата теории подстановок исследуются периодические свойства ґаммы, в частности проводится оценка вероятности появления ґаммы определенного периода при условии соответствия свойств шифра определенным свойствам случайной подстановки. Разрабатываются практические рекомендации по применению режима ґаммирования с обратной связью по шифрґамме, обосновываются требования и ограничения, вытекающие из полученных оценок периодических свойств ґаммы.

Ключевые слова: режим шифрования, периодичность ґаммы, случайная подстановка, Output Feedback. Табл.: 5. Ил.: 2. Библиогр.: 10 назв.

UDC 004.056.55

Periodic properties of the Output Feedback mode / A.A. Kuznetsov, Yu.I. Gorbenko, E.P. Kolovanova // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 239–251.

The properties of the Output Feedback mode are investigated in this paper. Periodic properties are investigated using the mathematical apparatus of permutations theory. In particular, estimating the probability of occurrence of a specified period gamma is performed, when the properties of the cipher meet certain properties of a random permutation. Practical recommendations for using the Output Feedback mode are developed. Requirements and restrictions arising from of the above estimates of the periodic gamma properties are justified.

Keywords: encryption mode, sequence period, random permutation, Output Feedback.

Tab.: 5. Fig.: 2. Ref.: 10 items.

ЭЛЕКТРОННЫЕ ДОВЕРИТЕЛЬНЫЕ УСЛУГИ И ИХ РЕАЛИЗАЦИЯ

УДК 681.3.06(07)

EIDAS: ПРИНЦИПЫ ПРЕДОСТАВЛЕНИЯ ДОВЕРИТЕЛЬНЫХ ЭЛЕКТРОННЫХ УСЛУГ И ПРОБЛЕМА ИНТЕРОПЕРАБЕЛЬНОСТИ

*А.В. ПОТИЙ, Ю.И. ГОРБЕНКО, А.В. КОРНЕЙКО, Ю.Н. КОЗЛОВ,
А.И. ПУШКАРЕВ, И.Д. ГОРБЕНКО*

В работе на основе анализа законодательства ЕС формулируется система принципов предоставления электронных доверительных услуг. Рассматриваются принципы электронной идентификации и принципы предоставления электронных доверительных услуг. Отдельно рассматриваются проблемы интероперабельности в данной сфере, а также подход европейских организаций к стандартизации и решению вопросов технической интероперабельности.

Ключевые слова: электронная идентификация, электронные доверительные услуги, интероперабельность.

ВВЕДЕНИЕ

Нет сомнений в том, что в Украине начинает формироваться существующий рынок электронных услуг. И хотя мы не найдем определения понятия «электронная услуга», их предоставление и использование уже регулируются рядом законов и подзаконных актов в различных сферах. Электронные платежи, осуществления финансовых операций с помощью Интернет-банкинга, открытие депозитов и оформление кредитов online, подача отчетных документов (деклараций, финансовой отчетности и пр.) в электронном виде и многое другое — все это можно назвать «электронной услугой». Все эти «электронные услуги» регулируются законами в банковской сфере, в сфере электронной цифровой подписи и иных сферах [4, 5, 6]. Уже появилась законодательная инициатива по принятию закона «Об электронной торговле», а там не за горами и настоящее регулирование электронного рынка Украины.

ЕС имеет большой опыт формирования и регулирования подобного рода вопросов и изучение этого опыта является важным и полезным для нашего государства, учитывая подписанные документы политической и экономической ассоциации Украины с ЕС. С содержанием Регламента [1] можно познакомиться на сайте XXXX. С анализом положений данного документа можно ознакомиться в работе [7].

В настоящей работе авторы делают попытку формирования системы принципов, лежащих в основе электронной идентификации и предоставления электронных доверительных услуг, опираясь на материалы конференции, проведенной в июне 2014 в Польше (European Forum on Electronics Signature (EFPE 2014). — Miedzyszdroje, Poland. — www.efpe.pl). Также в работе анализируются проблемы интероперабельности в сфере электронных услуг.

1. ЦЕЛЬ, ЗАДАЧИ И ФУНКЦИИ РЕГЛАМЕНТА

Итак, вы законопослушный гражданин и добросовестный налогоплательщик, который ежегодно представляет в налоговый орган свою декларацию. Государство, в лице налоговой администрации, заинтересовано в создании максимально комфортных условий для организации этого процесса, а также для упрощения порядка подачи деклараций гражданами. Нет ничего лучше, когда подача декларации будет осуществляться без непосредственного контакта представителя налоговой администрации и налогоплательщика. Еще лучше, когда у налогоплательщика будет возможность подать декларацию в любое удобное для него время и в любом удобном ему месте (дома, в офисе, в заграничной командировке, на пляже под ласковым солнцем). Реализация этого процесса в виде совокупности электронных транзакций позволяет предложить налогоплательщику такую удобную публичную электронную услугу. На рис. 1 как раз и представлена такая услуга. Результатом этой услуги является поданная налогоплательщиком и принятая налоговой администрацией налоговая декларация.

Удобно? Да, несомненно. Но есть, как говорится, вопросы. Как убедиться в том, что вы загрузили сайт именно налоговой администрации? А может его подменили? Вы уверены в том, что никто кроме Вас не сможет войти в Ваш персональный кабинет и сформировать отчетность? Вы уверены в том, что при формировании декларации и ее регистрации в налоговом органе она не будет модифицирована (подделана), даже уполномоченным сотрудником налоговой администрации? Вы доверяете этому обезличенному сотруднику или даже роботу по приему деклараций? Вы уверены, что налоговый орган получил Вашу декларацию? А Вам не скажут, что Вы нарушили сроки подачи декларации или вообще ее

не подавали? И как доказать свою правоту, если Вас в этом обвинят? А как и где эта декларация будет храниться? А можно ли ее будет получить в виде твердой копии? Вы уверены, что ее не опубликуют в Интернете? Вы уверены...? Вы доверяете...? Таких вопросов у каждого пользователя может быть тысяча, ведь мы все сомневаемся и такие консервативные.

Заметим, что скорее всего обычный гражданин мало будет беспокоиться о технических средствах реализации этого процесса, он просто не будет их замечать, поскольку мы стремимся сделать такой и подобные процессы максимально комфортными, прозрачными, нетрудоемкими. Основной вопрос, который всегда будет волновать гражданина это ДОВЕРИЕ (trust) к услуге и УВЕРЕННОСТЬ (confident) в ее безопасности. И без обеспечения этих краеугольных качеств нельзя говорить о полноценном рынке электронных услуг. Именно это является основной целью Регламента – укрепление единого Европейского рынка электронных услуг путем поддержки доверия и уверенности в безопасности, а также прозрачности трансграничных электронных транзакций [2].

Положения Регламента охватывают две основные сферы: *электронная идентификация и электронные услуги*.

В области *электронной идентификации* Регламент определяет условия взаимного признания странами ЕС средств электронной идентификации физических и юридических лиц, выданных в рамках национальных нотифицированных схем электронной идентификации. Это формирует правовую, организационную и технологическую основы трансграничной идентификации и аутентификации в странах ЕС, как минимум для публичных электронных услуг.

В сфере *электронных услуг* Регламент определяет правила предоставления квалифицированных доверительных электронных услуг, к которым относятся:

- услуги выпуска и управления сертификатов открытых ключей для поддержки электронной подписи и электронной печати;
- услуги по проверке (валидации) электронной подписи и печати;
- услуги по предоставлению метки времени;
- услуги по подтверждению подлинности (аутентификации) веб-сайтов;



Рис. 1. Услуга предоставления электронной декларации

— услуги по регистрации и подтверждению доставки электронных документов;

— услуги по безопасному хранению (в том числе архивному) подписанных электронных документов.

По сути Регламент формирует условия приемлемости электронных документов в отношениях между различными субъектами и взаимного признания электронных доверительных услуг, предоставляемых провайдерами, на всей территории ЕС.

Основные задачи, на решение которых направлено принятие и последующее внедрение положений Регламента, можно сформулировать следующим образом:

1. Обеспечение правовой определенности и основ для использования электронной идентификации гражданами ЕС, формирование культуры использования средств электронной идентификации и электронных услуг в повседневной жизни.

2. Формирование правовых основ для разработки и широкого внедрения набора механизмов и услуг по поддержке доверия и уверенности в безопасности электронных транзакций, в том числе и трансграничных.

3. Внедрение практики управления рисками, опирающееся на следующие принципы:

— прозрачность и наблюдаемость: четкое определение обязанностей провайдеров доверительных услуг (Trusted Service Provider) и установление их ответственности;

— доверительность услуг на основе выполнения провайдерами установленных требований безопасности;

— поднадзорность деятельности провайдеров доверительных услуг по предоставлению доверительных электронных услуг;

— технологическая нейтральность: исключение требований, которые могут быть удовлетворены специальными технологиями и техническими методами;

— стандартизация и единые правила технического регулирования.

4. Формирование единого набора правил предоставления доверительных электронных услуг, применимых для всех стран членов ЕС.

Принятие и внедрение положений Регламента будет играть важную роль в различных сферах общественной жизни.

В *правовой сфере* Регламент формирует надежный правовой фундамент предоставления доверительных электронных услуг с полноценной защитой прав потребителей на территории всех стран членов ЕС, с общими правилами предоставления этих услуг провайдерами на основе взаимного признания электронной идентификации.

В *экономической сфере* Регламент способствует формированию и развитию свободного единого Европейского рынка продуктов и дове-

рительных электронных услуг на основе общих правил Регламента.

В *социальной сфере*, путем формирования доверия и уверенности в безопасности через обеспечение свободы выбора в едином рынке электронных услуг, обеспечивается больший комфорт для граждан ЕС при осуществлении электронных транзакций.

В *технологической сфере* Регламент формирует основы для создания единой инфраструктуры электронного (цифрового) рынка и рынка электронных услуг, объединяющей в себя инфраструктуру электронной идентификации, инфраструктуру открытых ключей (PKI) и полномочий, органично вписывающейся в иные информационные инфраструктуры (в том числе и критические) стран-членов ЕС.

2. БАЗОВЫЕ ПРИНЦИПЫ ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ

Говоря об электронной идентификации (eID), мы будем учитывать следующие аспекты.

Во-первых, eID — это идентификация физических и юридических лиц путем выдачи им в установленном законом порядке и на основе установленной *схемы* специальных персональных средств электронной идентификации (электронных карточек, паспортов и проч., т.е. электронных идентификаторов, связанных с конкретным лицом).

Во-вторых, eID — это обеспечение технологической возможности осуществления аутентификации (подтверждения подлинности) владельца электронного идентификатора при выполнении им каких-либо электронных транзакций.

Эти два аспекта являются обязательными для предоставления электронных услуг и осуществления электронных транзакций. Регламент определяет базовые принципы электронной идентификации, которые рассматриваются ниже.

1. *Принцип взаимного признания.* Страны ЕС должны признавать средства электронной идентификации, которые выпущены в соответствии с национальными требованиями в рамках «нотифицированных» схем. Взаимное признание призвано способствовать трансграничному доступу к публичным электронным и иным услугам, требующих электронной идентификации. Таким образом, Регламент не вводит требования создания единой общеевропейской схемы электронной идентификации. Каждая страна формирует свою национальную инфраструктуру электронной идентификации.

2. *Принцип нотификации схемы электронной идентификации.* Страны ЕС обязаны уведомить Европейскую комиссию о национальных схемах электронной идентификации, которые используются на территории страны. Для этого определяются общие условия, формат и процедуры нотификации национальных схем.

3. *Принцип предоставления гарантий безопасности.* Нотифицированная схема электронной идентификации должна предоставлять определенный уровень гарантий безопасности (assurance level) средств электронной идентификации. Определены три уровня гарантий:

а. Низкий (low) уровень гарантий, который предполагает добровольное взаимное признание средств;

б. Достаточный (substantiation) уровень гарантий;

в. Высокий (high) уровень гарантий.

Последние два уровня гарантий предполагают обязательное (мандатное) признание. Спецификация требований гарантий будет базироваться на результатах работы в рамках проекта STORK (XXX) или требованиях международного стандарта ISO/IEC 29115 [16]. Можно предположить, что требования гарантий средств электронной идентификации будут согласовываться с требованиями гарантий Единых критериев ISO/IEC 15408 [14].

4. *Принцип интероперабельности нотифицированных схем электронной идентификации.* Обеспечение интероперабельности является одним из основных требований при реализации трансграничных электронных транзакций и предоставлении публичных электронных услуг. Комплексное решение проблемы интероперабельности направлено на устранение «электронных барьеров» для публичных услуг Евросоюза, построение «бесшовного» электронного пространства и единого электронного рынка.

5. *Принципы аутентификации.* Аутентификация должна базироваться на принципах безвозмездности предоставления услуги аутентификации, трансграничности и отсутствия дискриминации. Страны члены ЕС должны обеспечить возможность трансграничной онлайн аутентификации на основе электронной идентификации (eID-аутентификация). Трансграничная eID-аутентификация должна предоставляться публичной администрацией (уполномоченным государственным органом) на безвозмездной основе. Трансграничность и отсутствие дискриминации предполагает, что режимы и процедуры аутентификации в национальном приватном секторе должны быть применимы без каких-либо ограничений в приватном секторе других стран-членов ЕС. По сути, эти требования требуют согласования бизнес-процессов в рамках единого рынка ЕС.

6. *Принцип кооперации.* Кооперация предполагает обмен опытом и хорошей практикой применения средств электронной идентификации и аутентификации между странами членами ЕС.

7. *Принцип ответственности.* Принцип ответственности предполагает установление ответственности стран-членов ЕС, провайдеров услуг электронной идентификации и аутентификации за возможное нанесение ущерба в ходе

предоставления услуги электронной идентификации. Одним из направлений реализации этого принципа является страхование рисков в данной сфере.

3. ПРИНЦИПЫ ПРЕДОСТАВЛЕНИЯ ЭЛЕКТРОННЫХ ДОВЕРИТЕЛЬНЫХ УСЛУГ

Как отмечалось выше, Регламент регулирует деятельность в сфере предоставления электронных услуг. На наш взгляд принципиальным является то, что Регламент формирует основу рынка электронных услуг и переводит, например, электронную цифровую подпись из статуса уникальной технологии, в категорию одной из многих возможных электронных услуг свободно предоставляемых на рынке. Кроме того, перечень таких услуг будет расширяться по мере развития рынка и заинтересованности в таких услугах потребителей. Сейчас можно говорить, что закладываются основы формирования некой инфраструктуры единого рынка электронных услуг, которая будет интегрировать инфраструктуру открытого ключа, инфраструктуру электронной идентификации и другие «инфраструктуры». Регламент в явном виде определяет такие услуги:

- услуги выпуска и управления сертификатов открытых ключей для поддержки электронной подписи и электронной печати;
- услуги по проверке (валидации) электронной подписи и печати;
- услуги по предоставлению метки времени;
- услуги по подтверждению подлинности (аутентификации) веб-сайтов;
- услуги по регистрации и подтверждению доставки электронных документов;
- услуги по безопасному хранению (в том числе архивному) подписанных электронных документов.

Перечень услуг будет расширяться, например, уже сейчас рассматривается возможность предоставления услуги электронного апостиля.

Для широкого распространения электронной услуги, необходимо дать потребителю четкое и ясное ее определение, а также указать на те полезные эффекты (или выгоды), которые получит потребитель от использования данной услуги. В ряде исследований указывается на недостаточный уровень мотивации потребителя по использованию этих услуг [19]. Задача государственных органов, с одной стороны, и свободного рынка, с другой стороны, и заключается в формировании такой мотивации и распространения электронных услуг в приватном и публичном секторах.

Основным принципом предоставления электронных услуг является принцип **ДОВЕРИЯ**. Электронные услуги предоставляются *третьей доверительной стороной-провайдером доверительной услуги*. Доверительная третья сторона (ДТС) – это независимая организация, предоставляющая электронные услуги, которой доверяют пользователи на основе выполнения ДТС

определенных действий безопасным образом [14]. Регламент определяет два типа провайдеров доверительных услуг (trusted service provider-TSP) – квалифицированный (QTSP) и неквалифицированный. Отличаются они по уровню ответственности, надзору за их деятельностью и ограничениям, которые накладываются на их деятельность.

Принцип ответственности провайдера. Любой провайдер электронных доверительных услуг несет ответственность за нанесение ущерба, наступившего в результате его умышленных или неумышленных действий. Причем, изменение (установление) меры ответственности для QTSP возможны только в судебном порядке, в то время как для неквалифицированных TSP уровень ответственности является объектом договорного урегулирования с пользователем. На ответственность провайдеров распространяется принцип применимости национальных правил взыскания ущерба.

Принцип признания TSP третьих стран предполагает, что провайдеры доверительных электронных услуг третьих стран (не членов ЕС) могут быть признаны только через соответствующее международное соглашение между Еврокомиссией и третьей стороной или международной организацией, при обязательном соблюдении принципа отсутствия дискриминации.

Принцип доступности услуги провайдера для лиц с ограниченными возможностями (физическими недостатками).

Регламент определяет необходимость организации и осуществления надзора за деятельностью TSP и формирования соответствующих органов надзора. При этом для неквалифицированных TSP вводится реактивный мониторинг (т. е. контроль по факту (ex post) инцидента или облегченный надзор). А для QTSP вводится полноценный предварительный (ex ante) надзор и надзор по факту. Регламент определяет перечень задач органов надзора, правила взаимодействия национальных органов надзора между собой и с Еврокомиссией.

Регламент накладывает ряд обязательств на провайдеров электронных услуг. Для всех провайдеров вводятся минимальные требования по безопасности, в том числе требования по анализу уязвимостей. Для QTSP вводятся дополнительные требования безопасности, предъявляемые к персоналу, надежности (гарантоспособности) систем, эксплуатируемых провайдером, к схемам страхования ответственности, к порядку первой идентификации держателя сертификатов и т.д.

Подтверждение соответствия этим и иным требованиям квалифицированный провайдер получает в ходе аккредитации, в результате успешного прохождения которой, он вносится органом надзора в список квалифицированных провайдеров доверительных услуг. Ежегодно, не менее одного раза, провайдер доверительных

услуг должен проходить проверку, по результатам которой орган по надзору может исключить провайдера из списка. Орган надзора является держателем реестра квалифицированных провайдеров доверительных электронных услуг и реестра квалифицированных доверительных услуг, предоставляемых провайдерами. Для индикации квалифицированных доверительных услуг внедряется единая Европейская метка доверия (EU trustmark). Она используется квалифицированными провайдерами и в простой, легко-узнаваемой и ясной форме указывает на квалифицированный статус доверительной услуги, предоставляемой провайдером.

Требования и условия предоставления конкретных услуг достаточно подробно рассмотрены в работах [8,9].

4. ПРОБЛЕМА ИНТЕРОПЕРАбельНОСТИ ПУБЛИЧНЫХ ЭЛЕКТРОННЫХ УСЛУГ: КОНЦЕПТУАЛЬНЫЙ ПОДХОД К РЕШЕНИЮ

В контексте инфраструктуры доверительных электронных услуг, на проблему интероперабельности необходимо смотреть гораздо шире, чем просто как согласование форматов данных, протоколов и технических спецификаций средств электронной идентификации, ЭЦП и т.п.

«Интероперабельность – это способность несопоставимых и различных организаций взаимодействовать в интересах взаимной выгоды и согласования общих целей, путем распределения общей информации и знаний между организациями, через бизнес процессы, которые они поддерживают, посредством обмена данными между соответствующими информационно-телекоммуникационными системами.

Интероперабельность публичных электронных услуг является ключевым фактором формирования единого цифрового рынка Европы и обеспечения прозрачного трансграничного обмена информацией, что позволит гражданину и бизнесу воспользоваться всеми преимуществами свобод единого европейского рынка» [10].

Для решения проблем интероперабельности при внедрении схем электронной идентификации и публичных электронных услуг, европейская комиссия по коммуникациям разработала Европейскую стратегию по обеспечению интероперабельности (European Interoperability Strategy – EIS). В рамках этой стратегии реализуется программа «Интероперабельность Европейских публичных услуг», которая включает в себя ряд проектов и инициатив. Одной из такой инициатив является European Interoperability Framework (EIF, www.ec.europa.eu/isa/documentations/isa_annex_ii_eif_en.pdf).

Основная цель усилий в рамках этой инициативы является разработка общих методологических подходов к обеспечению интероперабельности администраторов (провайдеров)

публичных электронных услуг — т.е. услуг, которые предоставляются национальными государственными органами гражданам и бизнесу.

Интероперабельность играет важную роль в поддержание единого электронного рынка Европы. Всё возрастающее использование гражданами и бизнесом возможностей и свобод единого рынка Европы является основной причиной взаимодействия граждан и бизнеса с публичными администрациями за пределами своих национальных государств. Гражданам необходим постоянный доступ к информации и документам для работы, учебы и путешествий в странах ЕС. Деловым партнерам необходима информация для эффективного взаимодействия с партнерами из различных стран. На пути эффективного решения этих повседневных задач возникают *электронные барьеры* и причины их возникновения лежат не только в технической плоскости. Интероперабельность позволяет провайдерам публичных электронных услуг обмениваться информацией и взаимодействовать между собой для эффективного предоставления трансграничных электронных услуг.

Таким образом, интероперабельность позволяет обеспечить:

- взаимодействие между провайдерами публичных электронных услуг;
- обмен информацией между провайдерами для наиболее полного удовлетворения правовых требований и политических обязательств;
- распределение и совместное использование провайдерами публичных электронных услуг информации с целью повышения административной эффективности и устранения электронных барьеров для граждан и бизнеса.

В основе понимания и формулировки путей решения проблемы обеспечения интероперабельности лежит трехуровневая модель предоставления публичных электронных услуг (рис. 2) [10].

Агрегирование предполагает объединение публичных услуг в единый сервис для пользователей (государственных органов, бизнеса и граждан) и координацию действий провайдеров публичных услуг. При этом предполагается, что электронные транзакции будут трансграничными и осуществляются между различными административными и корпоративными уровнями через механизмы, удовлетворяющие специфическим бизнес-требованиям. Публичные услуги не должны предоставляться исключительно правительственными web-сайтами. Они должны легко интегрироваться в web-приложения посредников, но при этом ответственность за услугу не снимается с государственного органа. Необходимо реализовать четкую и ясную идентификацию, на основе которой пользователи однозначно различают публичную и приватную услуги.

На втором уровне решаются проблемы защиты данных и управления безопасностью. Вся публичная информация подлежит защите и должна соответствующим образом контролироваться. Безопасность потенциально является основным барьером к обеспечению интероперабельности, если требования безопасности не будут гармонизированы между организациями.

Уровень базовых публичных услуг определяет основные компоненты, на основе которых могут быть построены публичные электронные услуги.



Рис. 2. Трехуровневая модель предоставления публичных электронных услуг

Во-первых, это всевозможные электронные реестры (регистры), под которыми понимают надежные источники информации, находящиеся под управлением различных государственных администраций. К таким реестрам можно отнести реестр недвижимости, земельный кадастр, реестры лицензиатов и т.д. Эти реестры должны быть доступны для широкого и многократного использования при соблюдении требований безопасности информации и приватности.

Во-вторых, вводится понятие посредник интероперабельности (Interoperability Facilitators), который является провайдером таких услуг, как трансляция между протоколами, форматами данных и языками или действует как информационный брокер.

И, наконец, внешние услуги, например, электронные платежи или коммуникационные услуги.

На практике интероперабельность рассматривается на четырех уровнях: правовом, организационном, семантическом и техническом.

Правовая интероперабельность. Каждый национальный публичный орган предоставляет публичные электронные услуги в рамках национального законодательства и несовместимость законодательства стран-членов ЕС может существенно затруднить совместную работу органов в сфере предоставления публичных электронных услуг.

Организационная интероперабельность. Кооперация различных организаций направлена на интеграцию бизнес процессов и удовлетворение требований пользователей (потребителей) через обеспечение наблюдаемости услуг, легкости использования услуг, доступности услуг и ориентированности на конечного пользователя. Объектами организационной интероперабельности являются:

- согласование (выравнивание) бизнес процессов;
- организационное (корпоративное) взаимодействие;
- управление изменениями.

Семантическая интероперабельность. Существующие различия в языковой, культурной, правовой и административной среде стран ЕС являются серьезными вызовами для обеспечения однозначного и точного взаимопонимания взаимодействующих субъектов и распознавания форматов обмениваемой информации.

Техническая интероперабельность предполагает согласование формализованных технических спецификаций при реализации публичных электронных услуг.

В качестве механизма достижения интероперабельности на рассмотренных выше уровнях предлагается использовать *соглашения по интероперабельности* (interoperability agreements). На правовом уровне соглашение по интероперабельности предполагает, что предоставление публичных электронных услуг осуществляется

либо на основе национального законодательства, включающего требования Европейских директив, перенесенных на национальный уровень, либо на основе дву- и многосторонних соглашений между субъектами отношений в сфере публичных электронных услуг.

Соглашение на организационном уровне могут применять форму MoUs (XXX) или SLA (XXX), которые уточняют обязательства для участников трансграничных процессов и определяют ожидаемый уровень услуг, поддержки процедур, взаимодействия и т.п.

Соглашения на семантическом уровне могут принимать форму справочных таксономий, схем, сводов правил, словарей данных, библиотек и т.д.

Соглашения на техническом уровне включают в себя интерфейсы, механизмы безопасности, спецификации услуг, форматы данных, коммуникационные протоколы и др.

В последнее время предпринимаются значительные усилия по обеспечению интероперабельности на всех уровнях. Особая активность наблюдается на техническом уровне. Большую организационную и техническую работу проводит Европейская организация по стандартизации (CEN) и Европейский комитет по телекоммуникациям (ETSI) [12]. На рис. 3 представлена рационализированная структура нормативных документов и стандартов в сфере доверительных электронных услуг, которая закреплена Мандатом по стандартизации M460 [13] или просто Мандат 460.

Анализ требований стандартов из комплекса представленных в M460 документов будет предметом наших дальнейших публикаций.

ВЫВОДЫ

1. Страны Европейского союза активно работают над формированием единого и свободного цифрового рынка или рынка электронных услуг. По сути создается инфраструктура электронной идентификации граждан, на основе которой формируется инфраструктура электронных трансграничных доверительных услуг. Электронная подпись становится одной из этих услуг. Регламент закладывает методологические основы формирования такого рынка с учетом обеспечения прав и свобод граждан стран членов ЕС.

2. Формирование украинского национального законодательства в сфере электронной цифровой подписи и электронных услуг должно проводиться с учетом и на основе Регламента. Уже на уровне разрабатываемых законов необходимо обеспечить правовую интероперабельность схем электронной идентификации и предоставления электронных доверительных услуг.

3. Актуальными являются исследования проблем обеспечения интероперабельности электронных доверительных услуг на различных уровнях с привлечением широкого круга экспертов и исследователей из различных сфер (право,

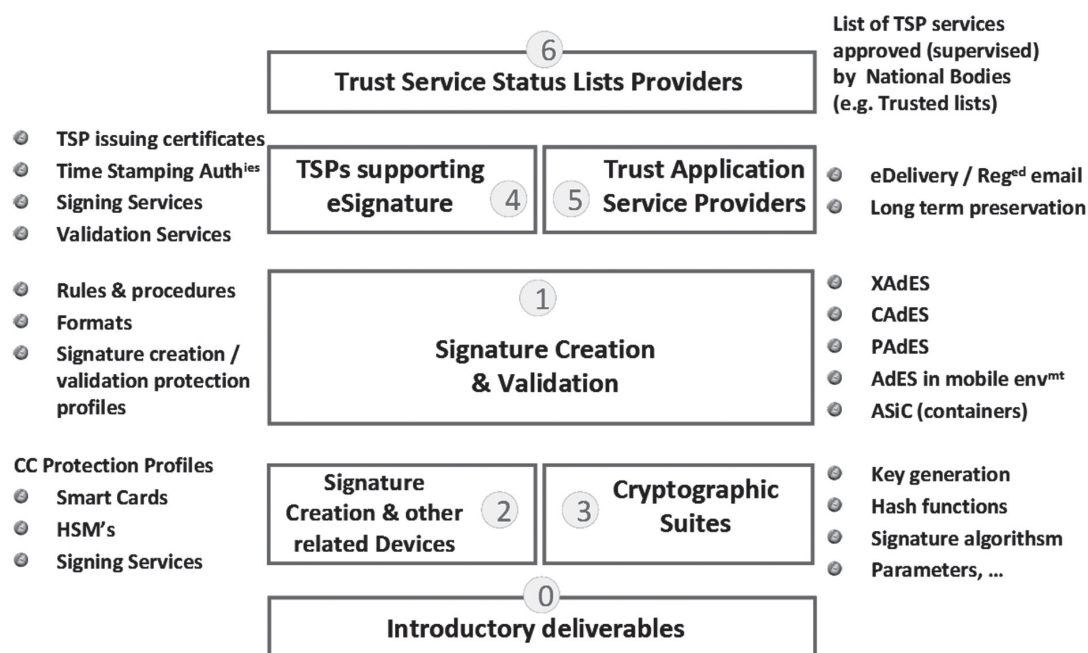


Рис. 3. Рационализированная структура стандартов, регулирующих технические вопросы в сфере электронных услуг (взято из доклада [12])

проектирование бизнес процессов, административное управление, бизнес администрирование, менеджмент, техническое регулирование). Украина должна приложить определенные усилия, чтобы отечественные специалисты были включены в различные группы и проекты, которые проводятся под руководством Европейской комиссии в этой сфере.

4. Ближайшей задачей разработчиков является анализ требований стандартов системы M460 и определения путей гармонизации стандартов с национальными стандартами в данной сфере. Наиболее рациональным подходом к гармонизации в данной сфере является гармонизация европейских стандартов методом обложки. В противном случае имеется риск отставания Украины от mainstream европейской стандартизации в данной сфере.

Литература

- [1] Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
- [2] Servida A. Draft Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) // European Forum on Electronics Signature (EFPE 2014). – Miedzydroje, Poland. – www.efpe.pl.
- [3] Директива Европейского парламента и совета Европы от 13.12.1999 о системе электронных подписей, применяющихся в границах Союза.
- [4] Закон України «Про електронний документ та електронний документообіг» №851-IV від 22.05.2003.
- [5] Закон України «Про електронний цифровий підпис». № 852-IX від 22.05.2003.
- [6] Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». №2594- IV від 31.05.2005 р.
- [7] Горбенко Ю.І. Сутність законодавчих основ та умови надання довірчих послуг в ЕС в період 2015-2030 рр. // Захист інформації. – Т.15, №2. – С. 164–174.
- [8] Горбенко Ю.І., Гончарова Ю.В. Електронна ідентифікація: поняття, визначення, вимоги // Радіотехніка. – Вип. 176. – 2014. – С. 138–144.
- [9] Горбенко Ю.І. Сутність та необхідність виконання додаткових вимог відносно надання довірчих послуг в ЕС та Україні в період до 2015-2030 років. // Радіотехніка. – Вип.176. – 2014. – С.145–152.
- [10] European interoperability Framework (EIF). Towards Interoperability for European Public Services // European Commission. – 2011.
- [11] Jon Ølnes. Technical aspects of the eIDAS regulation // European Forum on Electronics Signature (EFPE 2014). – Miedzydroje, Poland. – www.efpe.pl.
- [12] Arno Fiedler. EU eSignature Standards – making e-signatures (easy?) in the EU and beyond. Overview of the M/460 rationalisation executed so far and future challenges in the context of eIDAS Regulation // European Forum on Electronics Signature (EFPE 2014). – Miedzydroje, Poland. – www.efpe.pl.
- [13] Standardisation mandate m460 to CEN and ETSI on electronic signatures <https://ec.europa.eu/digital-agenda/en/news/standardisation-aspects-esignatures>.
- [14] ISO/IEC 14516 Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services.
- [15] ISO/IEC 15408-3 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.
- [16] ISO 29115:2013 Information technology – Security techniques – Entity authentication assurance framework.
- [17] Luca Castellani. The contribution of UNCITRAL texts on electronic commerce to cross-border electronic transactions: an European perspective. // European Forum on Electronics Signature (EFPE 2014). – Miedzydroje, Poland. – www.efpe.pl.

Поступила в редколлегию 15.05.2014



Потий Александр Владимирович, доктор технических наук, профессор, профессор кафедры безопасности информационно-телекоммуникационных систем Харьковского национального университета им. Каразина. Научные интересы: проектирование комплексных систем защиты информации, криптографических средств защиты информации; методы системного анализа процессов защиты информации; методы оценки безопасности объектов информационной деятельности.

Горбенко Юрий Иванович, фото и сведения об авторе см. на стр. 251.



Корнейко Александр Васильевич, кандидат технических наук, доцент, Первый заместитель Председателя Государственной службы специальной связи и защиты информации Украины. Научные интересы: криптографические системы и протоколы, проектирование и разработка систем, комплексов и средств криптографической защиты информации.



Козлов Юрий Николаевич, начальник отдела организации обеспечения услугами электронной цифровой подписи и сопровождения информационно-телекоммуникационной системы центрального удостоверяющего органа ГП «Информационный центр» Министерства юстиции Украины. Научные интересы: проектирование информационно-телекоммуникационных систем центров сертификации ключей; проектирование комплексных систем защиты информации в информационно-телекоммуникационных системах органов государственной власти; методы системного анализа процессов защиты информации; методы оценки безопасности объектов информационной деятельности.



Пушкарев Андрей Иванович, директор Департамента криптографической защиты информации Администрации Госспецсвязи Украины, лауреат Государственной премии Украины в области науки и техники. Научные интересы: криптографическая защита информации.

Горбенко Иван Дмитриевич, фото и сведения об авторе см. на стр. 216.

УДК 681.3.06(07)

EIDAS: принципи надання довірчих електронних послуг і проблема інтероперабельності / О.В. Потій, Ю.І. Горбенко, А.В. Корнейко, Ю.Н. Козлов, А.І. Пушкарьов, І.Д. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 252–260.

В роботі на основі аналізу законодавства ЄС формулюється система принципів надання електронних довірчих послуг. Розглядаються принципи електронної ідентифікації та принципи надання електронних довірчих послуг. Окремо розглядаються проблеми інтероперабельності в даній сфері, а також підхід європейських організацій до стандартизації щодо вирішення питань технічної інтероперабельності.

Ключові слова: електронна ідентифікація, електронні довірчі послуги, інтероперабельність.

Рис.: 3. Бібліогр.: 17 найм.

UDC 681.3.06(07)

EIDAS: principles of providing confidence electronic services and interoperability problem / A.V. Potiy, Yu.I. Gorbenko, A.V. Korneyko, Yu.N. Kozlov, A.I. Pushkarev, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 252–260.

The paper formulates a system of principles of providing electronic confidence service on the basis of analyzing the EU legislation. Principles of e-identification and those of providing electronic confidence services are considered. Interoperability problems in this area, as well as the approach of the European standardization organizations to standardization and solution of problems of technical interoperability are considered separately.

Keywords: electronic identification, electronic confidence services, interoperability.

Fig.: 3. Ref.: 17 items.

СОСТОЯНИЕ И СУЩНОСТЬ ПРОЦЕССОВ НОРМАЛИЗАЦИИ ЕВРОПЕЙСКОЙ НОРМАТИВНОЙ БАЗЫ В ОБЛАСТИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Ю.И. ГОРБЕНКО, А.В. ПОТИЙ, А.В. КОСТЕНКО, Е.В. ИСИРОВА, И.Д. ГОРБЕНКО

Рассматриваются процессы нормализации Европейской нормативной базы в области электронных подписей. Анализируются причины осуществления нормализации и результаты выполнения работ. Обсуждается новая схема нумерации документов, а также рассмотрена каждая из предметных областей применения.

Ключевые слова: нормализация европейской нормативной базы в области электронных подписей, электронные доверительные (трастовые) услуги, Мандат 460, структура нормативных документов в ЕС в области электронных подписей.

ВВЕДЕНИЕ

В Европейском Союзе (ЕС) уже 15 лет успешно внедряются и применяются электронные услуги. В соответствии с Директивой 1999/93/ЕС внедрена и успешно применяется электронная цифровая подпись (ЭЦП). Опыт ее применения позволил сделать положительные оценки, а также выявить проблемные вопросы, необходимость ее усовершенствования и развития. Также сделан вывод о необходимости расширении электронных услуг, сделать их в пределах ЕС трансграничными. Результаты исследований и разработок были представлены и утверждены в Регламенте 2012 года [1]. В 2014 году принят Регламент Европейского Парламента и Совета по вопросам электронной идентификации и доверительных услуг (сервисов) для электронных операций на внутреннем рынке (Регламент 2014) [2]. В данном документе расширяется сфера применения ЭЦП. Технология ЭЦП используется для предоставления электронных услуг метки времени и электронной печати. Кроме того, ЭЦП становится основным элементом подтверждения других электронных услуг — электронной идентификации, аутентификации, печати, электронного документа, надежной электронной доставки. В терминологии Регламента 2014 она получила название электронной подписи (ЭП). Широкое применение технологии ЭП обусловило разработку многочисленных стандартов и норм, затрагивающих различные вопросы реализации и использования ЭП. Это способствует унификации и обеспечению надежности средств ЭП. Однако наблюдается и негативный эффект — это несвязность многочисленных нормативных документов и стандартов, дублирование норм. Это, в свою очередь, усложняет ориентацию в массиве документов и корректное их применение разработчиками, регуляторами и сервис-провайдером электронных доверительных услуг и ЭП (рис. 1). Также формируются новые барьеры на пути дальнейшего расширения и применения электронных доверительных услуг. Все это

можно охарактеризовать некой «болезнью роста», когда система функционально усложняется и требует перехода на новую структуру, отвечающую степени функциональной сложности.

Целью настоящей статьи является анализ нормативного документа, который получил название Мандата 460, в части создания условий для взаимодействия разных систем ЭП на уровне ЕС посредством улучшенной рационализации существующей структуры нормативных документов.

1. СУЩЕСТВУЮЩАЯ СТРУКТУРА И ПРОЦЕСС НОРМАЛИЗАЦИИ НОРМАТИВНЫХ ДОКУМЕНТОВ В ОБЛАСТИ ЭЦП

На рис. 1 структура нормативных документов в области ЭП в ЕС в области ЭП до начала процессов нормализации приведена на рис. 1. Основной проблемой существующей структуры нормативных документов в области ЭП является обеспечение трансграничности даже внутри ЕС. Преодолевая эти и другие проблемы, было принято решение нормализовать и упорядочить нормативную базу.

Упорядочение или нормализация системы нормативных документов ЕС в области ЭП и электронных доверительных услуг осуществляется в рамках так называемого Мандата 460 [3]. Целью разработки и принятия Мандата 460 является создание условий для взаимодействия различных криптографических систем ЭП в ЕС. Эта цель достигается путем рационализации существующей структуры нормативных документов ЕС в области ЭП. Суть процесса нормализации приведена на рис. 2.

Можно увидеть, что множество документов классифицировано согласно определенным критериям. Процесс классификации позволил исключить дублирующие документы, а также дополнить систему недостающими документами. В результате такой классификации выделено семь групп документов. Каждая группа документов описывает определенный аспект применения

ЭП. На рис. 3 приводится рационализированная структура нормативных документов и стандартов ЕС в области ЭП и электронных доверительных услуг. Новая структура отражает систему документов от предоставления услуг в обобщённом виде, до конкретных систем, комплексов и средств.

Все нормативные документы и стандарты, по характеру норм и требований, делятся на 5 групп:

- руководства относительно ЭП;
- требования безопасности и политики безопасности;
- технические характеристики систем и средств ЭП;
- методы и инструментарии оценки соответствия требованиям;

Руководства относительно ЭП содержат рекомендации относительно функциональных решений в области (eSignature): рекомендации по выбору стандартов в определенном контексте реализации бизнес-процессов и связанных бизнес-требований, рекомендации по реализации требований стандарта (или серии стандартов), рекомендации по оценке реализации бизнес-требований и т.д.

Требования безопасности и политики безопасности. Этот тип документов определяет требования политики безопасности и требования безопасности для служб и систем, в том числе описывает стандартные профили защиты. Данные документы объединяют нормы и требования других технических стандартов безопасности, физические, процедурные и кадровые

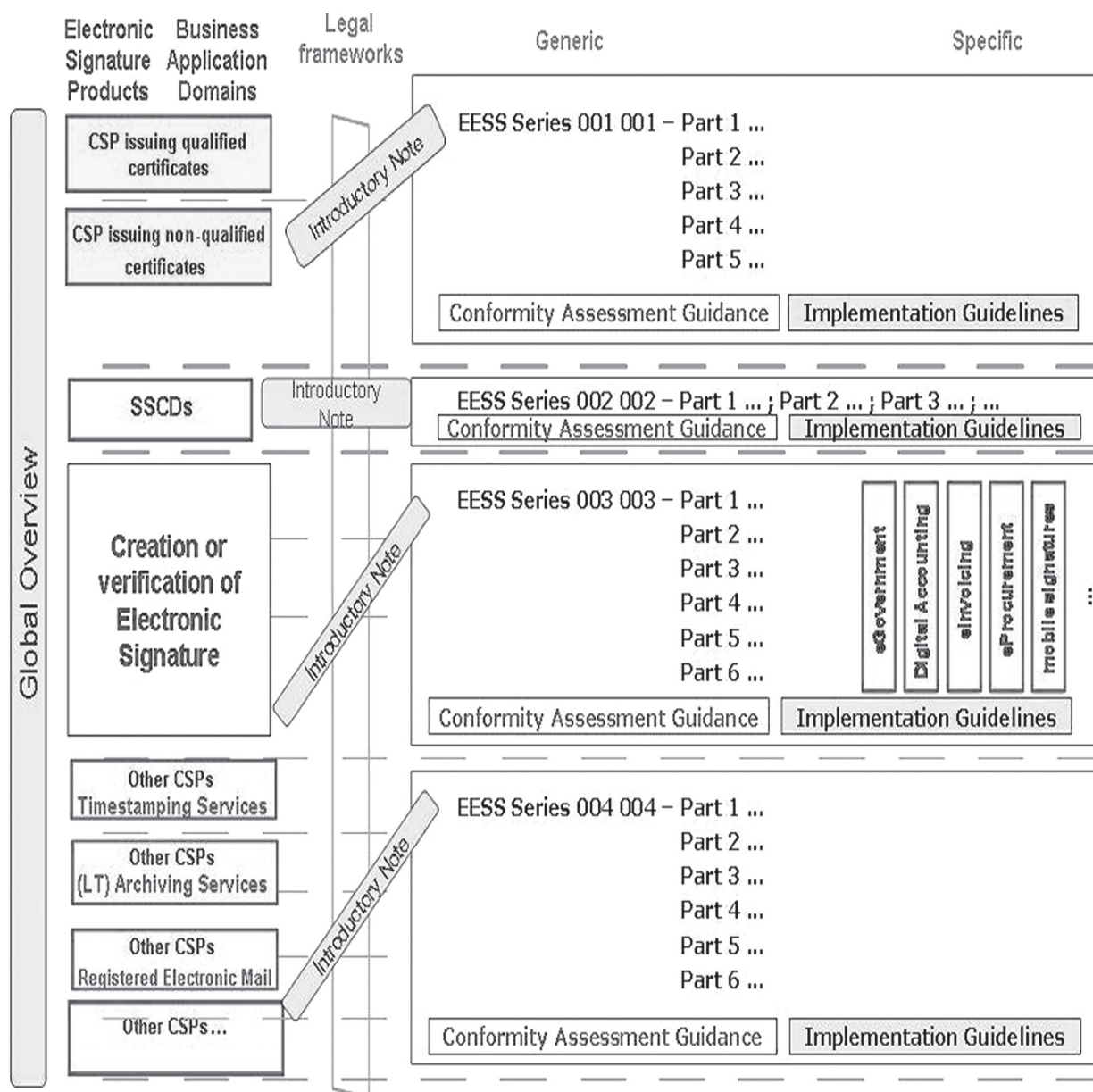


Рис. 2. Суть процесса нормализации нормативных документов в ЕС [4]

требования к системам, которые реализуют технические стандарты.

Технические характеристики систем. Эти документы определяют технические требования к системам и средствам ЭП. Они содержат форматы, протоколы, алгоритмы, API, профили конкретных стандартов и т.д., и не ограничиваются техническими архитектурами, которые описывают стандартизированные элементы системы и их взаимосвязи.

Требования к оценке соответствия требованиям стандартов описывают требования к оценке соответствия систем и средств ЭП требованиям безопасности. Документы содержат правила оценки соответствия, включая общие критерии оценки продукции или оценки систем и услуг и т.д.

Требования к тестовым испытаниям на совместимость. Эти документы содержат требования и спецификации для организации и проведения испытаний на совместимость, порядок



Рис. 3. Семиуровневая система нормативных документов в области ЭП [4]

тестирования систем, а также проведения испытаний или тестирования систем, которые обеспечивают автоматизированную проверку соответствия продукции, услуг или систем [4].

3. ОБОЗНАЧЕНИЕ ДОКУМЕНТОВ

Уникальная нумерация документации мандата 460 была выполнена с целью определения единого и последовательного ряда стандартов ЭП, и обеспечивает отслеживаемость всех модификаций документа за все время его существования.

В мандате 460 используется такая схема нумерации:

DD	L19	xxx	z
----	-----	-----	---

Поле DD указывает на тип соответствующего документа (принимает значения SR, TS, TR и EN);

Поле L19 — идентификатор составляющих частей документа. В данном идентификаторе L=4 — идентифицирует составляющую часть стандарта CEN. L=0, 1, 2 или 3 — идентифицирует составляющую часть стандарта ETSI и тип документа, который установлен в процессе стандартизации. Идентификатор 19 указывает на ряд документов по стандартизации, связанных с ЭП. Приняты следующие идентификаторы: код 019 — специальный отчет ETSI (SR); код 119 — техническая спецификация (TS) и технический отчет (TR) ETSI; код 219 — стандарт (ES) и руководство ETSI (EG); код 319 — Европейские нормы (EN) ETSI; 419 — техническая спецификация (TS) или Европейский стандарт (EN) CEN.

Поле xxx указывает серийный номер (от 000 до 999) документов ETSI/CEN. Первая цифра кода (Xxx) идентифицирует область документа: код 0 — общий для ряда областей; код 1 — создание руководства и проверка подписей; код 2 — устройства создания подписей; код 3 — криптографические комплексы; код 4 — провайдеры трастовых услуг, которые используют электронные подписи; код 5 — провайдеры приложений трастовых услуг; код 6 — список статуса провайдеров трастовых услуг.

Вторая цифра кода (xXx) определяет под-область в идентифицированной области, или 0 для общих документов данной области.

Третья цифра кода (xxX) обозначает тип документа, где: код 0 — руководства, код 1 — требования безопасности и политики безопасности, код 2 — технические характеристики, код 3 — оценка соответствия, код 4 — тестовые испытания и совместимость.

Поле z идентифицирует составные части документов.

Дополнительная нумерация для идентификации частей и версий будет осуществляться в соответствии с конвенциями ETSI или CEN в зависимости от того, какая организация публикует документ [4].

4. ХАРАКТЕРИСТИКА ГРУПП СЕМИУРОВНЕВОЙ СИСТЕМЫ ДОКУМЕНТОВ МАНДАТА 460

Рассмотрим подробнее документы, представленные в каждой из областей

Группа 0 — рационализированная структура. Данная группа объединяет документы, описывающие способы рационализации структуры документов и стандартов в сфере ЭП.

На первом этапе был проведен анализ существующей структуры документов. Далее выполняются такие работы:

- обновление документов, которые касаются рационализированной структуры;
- исследования на предмет расширения перечня документов (рис. 4).

Группа 1 — создание и проверка ЭП. Данная группа включает документы и стандарты, описывающие правила и процедуры создания и проверки ЭП, форматы ЭП, а также профили защиты приложений при создании и проверки ЭП.

На первом этапе были проведены «быстрые исправления» в действующих документах для исключения дублирования. Второй этап включает в себя разработку новых документов:

- руководства для бизнес-сферы (TR 119 100);
- политика требований для создания/проверки ЭП (TS 119 101);

Rationalised structure for Electronic Signature Standardisation						
Sub-areas						
Guidance						
TR	1	19	0	0	0	Rationalised structure for Electronic Signature Standardisation
TR	4	19	0	1	0	Rationalised structure for Electronic Signature Standardisation: Extended Rationalised structure including IAS
SR	0	19	0	2	0	Rationalised structure for Electronic Signature Standardisation: Rationalised Framework of Standards for AdES in Mobile environments
TR	4	19	0	3	0	Rationalised structure for Electronic Signature Standardisation: Best practices for SMEs
TR	4	19	0	4	0	Rationalised structure for Electronic Signature Standardisation: Guidelines for citizens
Policies						
TR	1	19	0	0	1	Rationalised Framework for Electronic Signature Standardisation: Definitions and abbreviations

Рис. 4. Документы группы 0 [5]

- профили защиты для приложений создания/проверки ЭП (EN 419 111);
- форматы ЭП (внесены изменения в существующие стандарты типа EN);
- процедуры создания/проверки ЭП (EN 319 102);
- политика ЭП (изменён стандарт TS 119 172);
- тестирование и интероперабельность: форматы ЭП (TS 119 1x4) и форматы политик (TS 119 174) [5].

Группа 2 – устройства создания ЭП. На первом этапе разработки данной группы документов были проведены обновления требований к профилям защиты с учётом пересмотра стандарта (EN 419 211). Согласно требованиям стандарта сервер ЭП должен выглядеть, как показано на рис. 5.

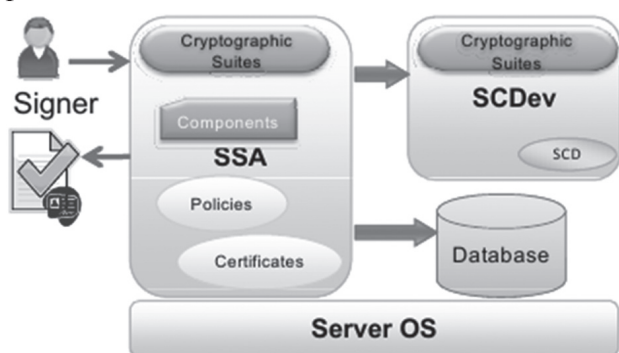


Рис. 5. Сервер подписи [5]

На последующих этапах работы были продолжены в таких направлениях:

- разработка стандарта метки времени (EN 419 231);
- разработка стандарта оценки и сертификации устройств создания подписей (EN 419 251);
- разработка стандарта SSSD интерфейса (EN 419 212).

В рамках этого направления работ также проходят исследования создания ЭП на мобильных устройствах и стандартизации требований для мобильных устройств.

Группа 3 – криптографические комплексы. В данную группу входят нормативные документы, которые описывают генерацию ключей, геш-функции, непосредственно алгоритмы ЭП и их форматы.

Первый этап нормализации завершился выходом обновленного стандарта TS 102 176-1.

На втором этапе был разработан и обновлен стандарт TS 119 312 – «Криптографические комплексы». В рамках данного стандарта был проведен анализ стойкости подписей на ближайшие 3–4 года, результаты которого приведены в табл. 1. Также разработаны руководства для использования ЭП в бизнес сфере (TR 119 300)[5].

Группа 4 – требования провайдеров доверительных электронных услуг. Основными работами по нормализации документов данной группы являются:

- разработка руководств (TR 119 400);
- оценка соответствия (Проект EN 319 403).

Также определены требования к провайдерам доверительных электронных услуг, которые используют ЭП. В результате пересмотрен стандарт «Общие требования» EN 319 401, пересмотрен стандарт «Квалифицированные сертификаты открытых ключей» EN 319 411, разработан проект стандарта «Сертификаты веб-сайтов» EN 319 411-1; разработан проект стандарта «Атрибуты сертификатов» EN 319 411-4; разработан проект стандарта «Метка времени» EN 319 421.

В дальнейшем планируется разработка нового объединенного стандарта «Сертификаты», который будет применяться для физических и юридических лиц, веб-сайтов, обеспечивая выпуск и обработку квалифицированных сертификатов.

Структура документов данной группы представлена на рис. 6.

Таким образом, можно выделить следующие тенденции стандартизации требований для провайдеров электронных доверительных услуг:

- 1) глобальное принятие стандартов для провайдеров электронных доверительных услуг в Европе, Северной Америке, Японии и т.д.;
- 2) необходимость оценки соответствия провайдеров по схемам, стандартизированным международными стандартами ISO 17065, 17021, 27006.
- 3) обеспечение регулярного пересмотра стандартов при наличии изменений в требованиях или важных условий.

Группа 5 – провайдеры приложений доверительных услуг. В этом направлении основные

Таблица 1

Анализ стойкости ЭП на ближайшие годы [5]

Entry name of the signature suite	1 years	3 years	6 years	10 years
sha256-with-rsa	1 536	2 048	2 048	not recommended
RSASSA-PSS with mgf1SHA-1Identifier	1 536	not recommended		
RSASSA-PSS with mgf1SHA-224Identifier	1 536	2 048	2 048	not recommended
RSASSA-PSS with mgf1SHA-256Identifier	1 536	2 048	2 048	3 072
sha224-with-ecdsa	224	224	not recommended	
sha256-with-ecdsa	256	256	256	256

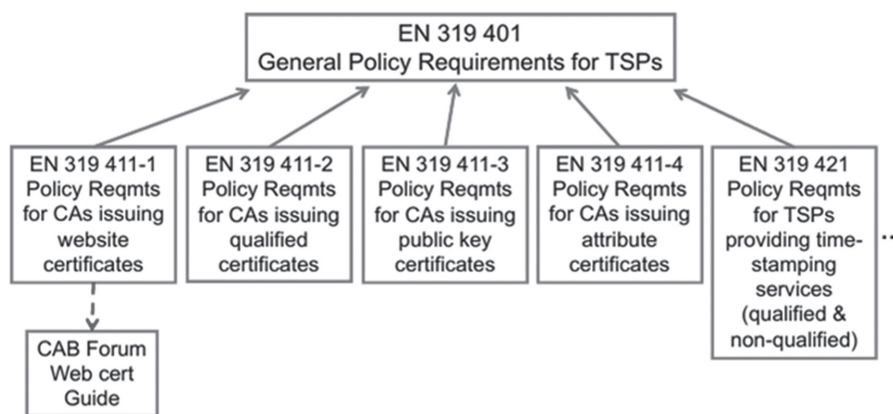


Рис. 6. Структура документов четвертой группы [5]

работы сводятся к разработке руководств для провайдеров (поставщиков) приложений доверительных услуг (TR 119 500) и исследованию необходимых аспектов внедрения стандартов электронной доставки (SR 019 530), а именно:

- обеспечение трансграничности услуги электронной доставки согласно Регламента-2014;
- внедрение стандартов идентификации отправителя;
- определение необходимого объема услуги электронной доставки.

На данный момент разработаны такие проекты стандартов:

- описание общей модели службы электронной доставки;
- анализ статуса стандартизации службы электронной доставки;
- предполагаемая структура стандартов.

Группа 6 – список статусов провайдеров электронных доверительных услуг. В соответствии с нормами Регламента 2014 в будущем должен быть сформирован список, который отражает статус провайдеров доверительных услуг, т.е. список доверия (trust list). Список является инструментом недопущения деятельности по предоставлению доверительных услуг провайдерами, которые не являются квалифицированными, а также инструментом предоставления актуальной информации обо всех доступных провайдерах электронных доверительных [2].

Основными направлениями стандартизации в этом направлении являются разработка «Руководства» (TR 119 600), разработка «Правил проверки соответствия провайдеров выдвинутым требованиям» (TS 119 614); разработка на формат списка доверия «Список доверия» (TS 119 612) [5].

ЗАКЛЮЧЕНИЕ

Таким образом, несмотря на многолетние исследования в ЕС и других технологически развитых государствах и союзах существует проблема нормализации нормативной базы в области электронных (цифровых) подписей. Ее разрешение даже на первом этапе позволит улучшить качество предоставляемых электронных доверительных услуг. Всем заинтересованным

сторонам, особенно разработчикам и пользователям будет легче ориентироваться в стандартах и нормативных документах. Также облегчиться контроль за исполнением требований действующего законодательства, появится возможность привлечения новых участников.

В целом, к сожалению, Мандат 460 только частично решает проблему законодательной путаницы. Тем не менее, на наш взгляд, необходимо для достижения конечного результата продолжать все начатые работы.

С точки зрения Украины участие в освоении, применении и совершенствовании этой нормативно-правовой базы позволит более оперативно двигаться к трансграничному электронному миру. Поэтому авторы надеются, что публикация этой статьи позволит рационально, и с лучшим качеством, решать возникшие проблемы.

Литература

- [1] Предложение Регламента Европейского парламента и Совета по вопросам идентификации и трастовых услуг для электронных операций на внутреннем рынке (2012).
- [2] Регламент Европейского парламента и Совета по вопросам идентификации и трастовых услуг для электронных операций на внутреннем рынке (2014).
- [3] Mandate M460: «Standardisation Mandate to The European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures».
- [4] Eesignature & Electronic Trust Services Standardisation Workshop-3rd December 2013 (Work Progress for Phase 2 of m460 Mandate).
- [5] Terms of Reference – Specialist Task Force 458 (TC ESI) Rationalised Framework for electronic signatures standards; Activities related to Signature Creation and Validation and Trusted Service Providers (TSP) supporting eSignatures.

Поступила в редколлегию 29.05.2014

Горбенко Юрий Иванович, фото и сведения об авторе см. на стр. 251.

Потий Александр Владимирович, фото и сведения об авторе см. на стр. 260.



Костенко Алексей Владимирович, заместитель начальника Управления функционирования центрального удостоверяющего органа Министерства юстиции Украины. Научные интересы: совершенствование законодательства и разработка совместных нормативно-правовых актов в сфере криптографической защиты информации и технической защиты информации.



Исирова Екатерина Владимировна, студентка 5 курса кафедры безопасности информационных систем и технологий ХНУ им. В. Н. Каразина. Научные интересы: защита информации в ИТС.

Горбенко Иван Дмитриевич, фото и сведения об авторе см. на стр. 216.

УДК 681.3.06(07)

Стан та сутність процесів нормалізації Європейської нормативної бази в області електронних підписів / Ю.І. Горбенко, О.В. Потій, О.В. Костенко, К.В. Ісірова, І.Д. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 261–267.

Розглядаються процеси нормалізації Європейської нормативної бази в області електронних підписів. Аналізуються передумови проведення процесу нормалізації та результати робіт. Обговорюється нова схема нумерації документів, а також розглянуто кожну із предметних галузей використання.

Ключові слова: нормалізація Європейської нормативної бази в області електронних підписів, електронні довірчі (трастові) послуги, Мандат 460, структура нормативних документів в ЄС в області електронних підписів.

Табл.: 1. Іл.: 6. Бібліогр.: 5 найм.

UDC 681.3.06(07)

The state and main point of normalization processes of European regulatory framework in the sphere of electronic signatures / Yu.I. Gorbenko, A.V. Potiy, A.V. Kostenko, E.V. Isirova, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 261–267.

The normalization processes of European regulatory framework in the sphere of electronic signatures are considered. The causes of the normalization processes and the results of the work done are analyzed. A new numbering scheme of documents is discussed and each of the subject areas of application is described.

Keywords: normalization processes of European regulatory framework in the sphere of electronic signatures, electronic trust services, Mandate 460, structure of European regulatory documents in the sphere of electronic signatures.

Tab.: 1. Fig.: 6. Ref.: 5 items.

АНАЛІЗ СТІЙКОСТІ ПОСТКВАНТОВИХ КРИПТОСИСТЕМ

Ю.І. ГОРБЕНКО, Р.С. ГАНЗЯ

В роботі наводяться оцінки стійкості популярних асиметричних криптосистем проти квантового криптоаналізу на основі алгоритму Шора, показано основні класи криптосистем, що будуть стійкими до квантового криптоаналізу на основі алгоритмів Шора та Гровера. Наводяться оцінки стійкості постквантових криптосистем проти класичного та квантового криптоаналізу.

Ключові слова: постквантова криптографія, алгоритм Шора, алгоритм Гровера, NTRU.

ВСТУП

Безпека сучасних інформаційних систем та технологій базується на стійкості криптографічних перетворень, які вони використовують для криптографічної обробки інформації. Так з використанням алгоритму Шора [1] складність криптоаналізу таких криптосистем як RSA, DSA, ECC буде поліноміальною, хоча з використанням класичних алгоритмів криптоаналізу, відомих на сьогодні, складність атаки на такі криптосистеми є субекспоненційною або експоненційною. Використовуючи алгоритм Гровера [2] можна зменшити складність атаки на симетричні криптосистеми та деякі криптосистеми на основі фактор-кілець.

Після винайдення Шором у 1994 році поліноміального алгоритму знаходження періоду функції велика кількість криптографів та математиків почали працювати у напрямку постквантової криптографії, тобто криптографії, яка існуватиме після появи квантового комп'ютера. На сьогодні вже існують певні класи криптосистем, які за своєю структурою будуть стійкими до квантового криптоаналізу на основі алгоритмів Шора та Гровера. Такі криптосистеми, як правило, презентуються та обговорюються на щорічній конференції PQCrypto з 2006 року. За останні роки вже було запропоновано певні класи криптосистем, що будуть стійкими до квантового криптоаналізу на основі алгоритмів Шора та Гровера [3–6].

1. ПОРІВНЯННЯ КЛАСИЧНОГО ТА КВАНТОВОГО АЛГОРИТМІВ КРИПТОАНАЛІЗУ СУЧАСНИХ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ

Квантові алгоритми Шора та Гровера для проведення криптоаналізу потребують квантовий комп'ютер, у якому поведінка системи кубітів визначатиметься законами квантової механіки, а також достатньо велику (на даний момент часу) кількість кубітів. Тривалий час можливості створення квантового комп'ютера були достатньо скептичні, але у 2007 році канадська компанія D-Wave презентувала свій 16-кубітний квантовий комп'ютер, а вже у 2013 році вона продала комп'ютер із 512 кубітами Google та NASA [7]. Тобто за достатньо невеликий проміжок часу

колектив дослідників компанії D-Wave досяг значних успіхів у збільшенні кількості кубітів на процесорі квантового комп'ютера.

Створенням квантового комп'ютера займаються багато наукових колективів, серед них такі, як: Каліфорнійський технологічний інститут, IBM, D-Wave Systems, Російський квантовий центр та Національний дослідницький технологічний інститут "MICS". Сьогодні кожний з колективів досяг значних успіхів у напрямку побудови такого комп'ютера, але найбільші результати залишаються за D-Wave, проте, як показує аналіз, комп'ютер D-Wave не підходить для реалізації алгоритмів квантового криптоаналізу, тому що на ньому не можуть бути реалізовані алгоритми, які використовують квантові вентиля. Тобто вважається, що ні алгоритм Шора, ні алгоритм Гровера на ньому не можуть бути реалізованими [7, 8]. Це пов'язано з тим, що для обчислень використовується зовсім інший принцип — так звані адиабатичні квантові обчислення. Вказане значно обмежує його можливості, але дозволяє не турбуватися про декогеренції та інші проблеми, що характерні для звичайних квантових обчислювачів.

Важливим є факт, що став відомим на початку 2014 року, на основі документів [8], наданих колишнім підрядником Агентства національної безпеки США (АНБ) Едвардом Сноуденом. Документи свідчать про те, що АНБ запустило дослідницьку програму, на яку виділено \$ 79,7 млн., під назвою "Проникнення до важких цілей" з метою розробки квантового комп'ютера, здатного зламати шифрування, що є уразливим для квантових комп'ютерів.

Зараз широке розповсюдження та застосування знайшли алгоритми асиметричного перетворення в кільці, в групі та в групі точок еліптичної кривої, прикладами таких криптосистем є RSA, DSA, ECC. Більшість атак на такі криптосистеми направлені на знаходження особистого ключа, так для криптосистеми RSA стійкість проти такої атаки базується на складності факторизації модуля перетворення N . Усі відомі сьогодні класичні алгоритми факторизації мають або експоненційну, або субекспоненційну складність. Вважається, що найкращим з точки зору мінімізації складності факторизації — є алгоритм

загального решета числового поля, або його модифікації. Часова складність таких алгоритмів оцінюється як субекспоненційна, наприклад, у вигляді [7]:

$$O(\exp(\delta + o(1)(\ln N)^\gamma (\ln \ln N)^{1-\gamma})), \quad (1)$$

$$\delta = 1.92, \gamma = 1/3.$$

Водночас квантовий алгоритм Шора має поліноміальну складність. Він здатен розкласти складене число на прості множники приблизно за час:

$$O(4n^3), \quad (2)$$

з використанням такої кількості кубітів:

$$O(2n), \quad (3)$$

де n — кількість бітів у розмірі модуля перетворення.

Пропозиція та оцінки складності алгоритму Шора вразили, пробудивши широкий інтерес до квантових обчислень. В алгоритмі Шора використано ефект квантового паралелізму, який запропоновано для отримання суперпозиції всіх значень функції за один крок. Після цього здійснюють квантове перетворення Фур'є функції. Подальші обчислення дозволяють визначити з великою ймовірністю період модуля перетворення, який використовується для його факторизації. З точки зору часу роботи алгоритму — більша його частина припадає на перетворення Фур'є, що базується на алгоритмі швидкого перетворення Фур'є [1].

Проведений аналіз показує [7], що алгоритм Шора дискретного логарифмування у групі точок еліптичної кривої та в скінченному полі має однакові кроки, єдине в чому відмінність — це представлення точок еліптичної кривої та елементів поля. Сьогодні вважають, що вирішення задач дискретного логарифмування у групі точок еліптичних кривих найбільш ефективно може бути реалізованим з використанням p - та λ -методів Полларда. Для них складність можна оцінити як:

$$O(\sqrt{q}), \quad (4)$$

де q — кількість точок еліптичної кривої.

Водночас квантовий алгоритм Шора у загальному випадку здатен розв'язати логарифмічне рівняння приблизно за такий час:

$$O(360n^3), \quad (5)$$

та з використанням такої кількості кубітів:

$$O(7n + 4 \log_2 n + 10), \quad (6)$$

де n — розмір базової точки.

Детальний порівняльний аналіз класичного алгоритму та квантового алгоритму Шора для розв'язку дискретного логарифму в групі точок еліптичної кривої наведено у [7]. Так навіть збільшення розміру порядку базової точки в ході криптоаналізу з використанням квантового алгоритму не дає суттєвого збільшення криптографічної стійкості. Також видно, що зі збільшенням модуля та порядку базової точки, склад-

ність дискретного логарифмування класичними методами в групі точок еліптичної кривої суттєво зростає.

Проте для квантового алгоритму проблемою є велика кількість кубітів, яка необхідна для проведення квантової атаки. Причому це залишається проблемним навіть в умовах появи квантових комп'ютерів, що здатні виконати алгоритм Шора. Вважається, що така велика кількість кубітів тривалий час буде недоступною. Саме на цьому і може базуватися стійкість таких систем, але це є лише тимчасовим шляхом вирішення проблеми.

Необхідно зазначити, що для забезпечення криптографічної стійкості перетворень у групі точок еліптичних кривих, бо саме таке перетворення використовується в національному стандарті ДСТУ-4145, у перспективі необхідно збільшувати розміри загальних параметрів з порядком базової точки навіть до 1024 бітів.

2. МОЖЛИВОСТІ ПРОТИДІЇ КВАНТОВОМУ КРИПТОАНАЛІЗУ

Основним напрямком протидії квантовим алгоритмам криптоаналізу є винайдення нових класів криптосистем, стійкість яких не ґрунтується на таких математичних проблемах як складність факторизації цілого числа чи розв'язку дискретного логарифму. Напрямок таких досліджень названо терміном постквантова криптографія, тобто криптографія, яка буде стійкою навіть після появи квантового комп'ютера, що матиме велику кількість кубітів для своєї роботи. Цей напрямок робіт популяризувався після 2006 року, саме тоді була проведена перша конференція за цією тематикою (PostQuantumCrypto 2006). Така конференція проводиться щорічно і збирає для обговорення найкращі здобутки за рік у напрямку постквантової криптографії.

Що стосується симетричних криптосистем, то більшість сучасних симетричних шифрів та геш-функцій захищені від квантових комп'ютерів. Квантовий алгоритм Гровера може прискорити криптоаналіз таких криптосистем, але йому можна протидіяти збільшенням розміру ключа чи блоку повідомлення [8]. Стилий аналіз можливостей алгоритму Гровера, щодо криптоаналізу симетричних криптосистем, буде наведено нижче.

Отже, враховуючи останні досягнення у напрямку постквантової криптографії, можна виділити такі класи криптосистем, що будуть стійкими до квантового криптоаналізу [3]:

- Криптографія на основі решіток.
- Мультиваріативна криптографія.
- Криптографія на основі геш-функцій.
- Криптографія на основі кодів.
- Криптографія ізогінеї суперсингулярних еліптичних кривих.
- Симетрична криптографія.

3. АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ КРИПТОГРАФІЇ НА ОСНОВІ РЕШІТОК У ПОСТКВАНТОВОМУ СВІТІ

Криптографія на основі решіток є новітнім класом альтернативних схем відкритого ключа і сьогодні є активною областю для досліджень. Є кілька складних проблеми, які можуть бути використані, щоб побудувати криптосистеми на базі решіток, найпопулярнішою є проблема знаходження найкоротшого вектора.

Цей напрямок включає в себе такі криптографічні системи, як NTRU та GGH. Згідно з Міссіансіо і Регева [5], криптографію на основі решіток можна розділити на дві категорії: практичні криптосистеми, такі як NTRU, які не володіють доказами безпеки таких схем, і теоретичні, такі як матриці на основі навчання з помилками (Learning with Errors, LWE), які пропонують сильні докази безпеки, але використовують ключі, які є занадто великими для загального використання. З 2008 року ведуться дослідження з об'єднання цих двох категорій, проте на сьогодні ще не вдалося об'єднати ці дві категорії і створити новий клас криптографічних систем на основі решіток, які б діяли ефективно як NTRU і були б доказово стійкими як LWE.

Протягом останніх років було запропоновано низку атак на криптосистему NTRU. Найкращою відомою класичною атакою є атака «зустріч посередині», що була запропонована в Одлижко у 2003 році, з використанням ідеї цієї атаки та квантового алгоритму Гровера у 2012 році була запропонована ефективна квантова атака на NTRU «зустріч посередині», яка в подальшому була удосконалена Вангом [8]. Аналітична часова і просторова складність таких атак наведена у табл. 1.

Таблиця 1

Аналітична складність атак на NTRU

	Класична атака «зустріч посередині»	Удосконалена квантова атака «зустріч посередині»
Часова складність	$O\left(\frac{C_{N/2}^{d/2}}{\sqrt{N}}\right)$	$O\left(C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor} \log C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor}\right) + \tilde{O}\left(\sqrt{C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor}}\right)$
Просторова складність	$O\left(\frac{C_{N/2}^{d/2}}{\sqrt{N}}\right)$	$O\left(C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor}\right)$

Детальний аналіз стійкості криптосистеми NTRU проти квантового та класичного криптоаналізу наведено у [8]. Результати досліджень показали, що хоча квантова атака і потребує менше операцій, проте вона вимагає все одно субекспоненційної кількості квантових гейтів для реалізації на реальні криптосистеми.

Отже криптографічні конструкції на основі решіток мають великі перспективи для свого використання в інформаційній сфері, так криптосистема NTRU вже стандартизована (стандарт

IEEE 1363.1) і використовується для надання послуги конфіденційності. Для України є важливим розвиток цього напрямку, враховуючи те, що ця криптосистема є стійкою до квантового криптоаналізу, має невеликі розміри загальносистемних параметрів і має великі швидкості зашифрування/розшифрування.

4. АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ КРИПТОГРАФІЇ НА ОСНОВІ ГЕШ-ФУНКЦІЙ У ПОСТКВАНТОВОМУ СВІТІ

Ядром такого класу криптосистем є те, що звичайні геш-функції використовуються як базові операції для генерації цифрових підписів, як правило, за допомогою направленої дерева графів. Така ідея була запропонована в 1979 році Лампортом [3, 5], він запропонував схему одно-разового підпису. Ідея Лампорта була покращена Вінтерніцом з метою забезпечення більш ефективного підписання великого обсягу даних. У 1989 році Меркле опублікував схему цифрового підпису на основі дерева геш-функцій для підвищення разових підписів, запропонованих Лампортом. Таку схему назвали схема підпису Меркле (MSS), вона дозволяє збільшити число підписів з використанням однієї зв'язки особистого та відкритого ключа, оскільки в двійковій системі геш-дерево сильно зменшується, необхідний обсяг пам'яті. Перевагою MSS є доказ її безпеки, що покладається тільки на безпеку використаної геш-функції. Недоліком такої схеми є обмежене число підписів, які можна виготовити з однією парою ключів. Ця проблема була вирішена побудовою декількох рівнів геш-дерев Меркле. Схеми підпису на основі геш-функцій адаптуються до різних сценаріїв застосування. Їх продуктивність, розміри ключів і розміри підпису залежить від того, яка геш-функція лежить в основі, максимальну кількість підписів та інші фактори можна регулювати для кожного випадку застосування криптосистеми окремо.

MSS має надзвичайно короткий відкритий ключ (довжина є виходом геш-функції, що лежить в основі), відносно велику довжину підпису, проте в цій схемі генерація ключів є обчислювально дорогою. Незважаючи на це, особистий ключ є досить великим, але його не обов'язково зберігати весь, його частина може бути згенерована «на льоту». Великим ступенем свободи для застосування такої криптосистеми є вибір геш-функції, що буде використана для виробки підпису. Можливі алгоритми, такі як SHA-1 або SHA-2 або будь-який алгоритм блокового шифрування. Таким чином, є багато варіантів конструкції криптосистеми на базі геш-функцій.

Оцінка стійкості таких криптосистем базується на складності криптоаналізу геш-функцій, які є ядром такої асиметричної криптосистеми. Ймовірність такої атаки складає 1/2, складність такої атаки для класичних комп'ютерів [3]:

$$O(2^{n/2}), \quad (7)$$

для квантових комп'ютерів:

$$O(2^{n/3}). \quad (8)$$

Порівняльний аналіз квантового та класичного криптоаналізу криптосистем на базі геш-функцій наведено в табл. 2.

Таблиця 2

Порівняльний аналіз стійкості криптосистем на базі геш-функцій проти класичного та квантового криптоаналізу

Вихідна довжина, біт	128	224	256	384	512
Класична атака, бітових операцій	2^{64}	2^{112}	2^{128}	2^{192}	2^{256}
Квантова атака, квантових гейтів	2^{43}	2^{75}	2^{86}	2^{128}	2^{171}

Отже стійкість такого класу криптосистем проти квантового криптоаналізу хоча і є менше, ніж проти класичного, але вона все одно має субекспоненційну складність. Отже, враховуючи існуючі недоліки такого класу криптосистем як обмежена кількість застосувань для одного набору ключів або побудова декількох рівнів дерев геш-функцій, є і переваги, а саме свобода вибору геш-функцій, які складатимуть ядро такої криптосистеми, а також велика швидкодія такої криптосистеми і невеликий розмір ключових даних. Стійкість такої криптосистеми залежить від того, яка геш-функція використовується, оскільки в Україні незабаром з'явиться національний стандарт геш-функції з розміром вихідних даних до 512 бітів, такий напрямок розвитку постквантових криптосистем є надзвичайно цікавим і для застосування в інформаційних системах на національному рівні, важливим аспектом є те, що такі криптосистеми будуть стійкими до квантового криптоаналізу [5].

5. АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ СИМЕТРИЧНОЇ КРИПТОГРАФІЇ У ПОСТКВАНТОВОМУ СВІТІ

Метод Гровера [2] вирішує задачу, яка може бути сформульована так: нехай дана неупорядкована база даних (список) з N елементів, і нехай в ній існує один елемент, що володіє деякою властивістю (яка легко перевіряється) і потрібно знайти цей елемент. Так алгоритм Гровера може бути застосований для криптоаналізу геш-функцій чи симетричних шифрів. З використання алгоритму Гровера можна знайти секретний ключ симетричного шифрування за час $\sqrt{K}$, де K – розмір ключа. Детальний опис стійкості симетричних систем проти квантового криптоаналізу наведено в табл. 3 та в роботі [8].

З табл. 3 чудово видно, що стійкість симетричних шифрів при атаці з використанням квантового алгоритму суттєво зменшується. Це означає, що DES може бути повністю скомпро-

метований і не можливо буде вважати його стійким, його стійкість дорівнюватиме 2^{28} . Навіть при AES бажано використовувати ключ 256 бітів. Тобто в цілому алгоритм Гровера, хоча і зменшує стійкість сучасних симетричних криптосистем, але все одно потребує субекспоненційної кількості квантових гейтів на відміну від алгоритму Шора.

Таблиця 3

Порівняльний аналіз стійкості симетричних криптосистем проти квантового криптоаналізу

Шифр	Стійкість при атаці на	
	блок повідомлення, квантових гейтів	ключ, квантових гейтів
AES-128	$2^{64} (10^{19,2})$	$2^{64} (10^{19,2})$
AES-256	$2^{64} (10^{19,2})$	$2^{128} (10^{38,4})$
DES	$2^{32} (10^{9,6})$	$2^{28} (10^{8,4})$
TDES	$2^{32} (10^{9,6})$	$2^{134} (10^{40,2})$
ГОСТ-28147	$2^{32} (10^{9,6})$	$2^{128} (10^{38,4})$
Калина-128	$2^{64} (10^{19,2})$	$2^{64} (10^{19,2})$
Калина-256	$2^{128} (10^{38,4})$	$2^{128} (10^{38,4})$
Калина-512	$2^{256} (10^{76,8})$	$2^{256} (10^{76,8})$
Blowfish	$2^{32} (10^{9,6})$	$2^{224} (10^{67,2})$

Таким чином бажано використовувати симетричні криптосистеми з розмірами загальносистемних параметрів більше 256 біт, в Україні незабаром буде прийнятий стандарт симетричного шифрування з можливими розмірами загальносистемних параметрів (блока повідомлення і ключа) 512 біт і таку криптосистему можна вважати стійкою до квантового криптоаналізу на основі алгоритму Гровера.

6. АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ ІНШИХ КЛАСІВ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

У 1978 р. Мак-Еліс запропонував схему шифрування з відкритим ключем на основі кодів, що виправляють помилки [5]. Ця криптосистема є однією з найбільш вивчених криптосистем з відкритим ключем на сьогодні. Криптосистема Мак-Еліса заснована на ідеї того, що існують ефективні декодери для деяких кодів, як, наприклад, коди Гоппа, але не для загальних лінійних кодів, для яких декодування є NP-важкою задачею. Після цього було запропоновано ще деякі криптосистеми, які базуються на такій ідеї, наприклад, криптосистема Niederreiter або деякі інші схеми підпису на основі кодів.

Основною операцією такої схеми з використанням кодів є множення матриці-вектора, що робить його дуже ефективним (насправді швидше, ніж більшість сучасних асиметричних схем). Основна операція під час розшифрування – це декодування кодів Гоппа над полем $GF(2^m)$, які, як правило, використовують розширений алгоритм Евкліда, який є ефективним для параметрів, що використовуються у схемі Мак-Еліса. Ключові розміри для безпечних наборів

параметрів змінюються від сотень кілобайт до мегабайт для особистого ключа. Генерація ключів залучає операцію інверсії матриці, яка також є ефективною. Таким чином, з практичної точки зору, криптосистема на основі кодів має такі особливості: швидке шифрування / розшифрування, великий рівень безпеки, але і мають свої недоліки: великі розміри ключів, накладні шифрування, дорогі з обчислювальної точки зору операції виготовлення підпису.

На таку криптосистему запропоновано низку різних атак, основним з них є груба сила, структурна атака, декодування набору інформації (та її квантова реалізація). У роботі [4] Бернштейном запропоновано квантову атаку декодування набору інформації і показано, що вона є набагато швидшою, ніж вважалося. Так в його роботі показано, що складність класичної атаки є:

$$c^{(1+o(1))n/\log_2 n}, \quad (9)$$

а квантової:

$$c^{(1/2+o(1))n/\log_2 n}, \quad (10)$$

де

$$c = 1/(1-R)^{(1-R)}. \quad (11)$$

Коди задаються набором параметрів (n, k, t) і тоді $R = k/n$ (швидкість коду). Код з характеристиками (1024, 524, 50) був зламаний і зараз треба використовувати більші параметри, наприклад, (4096, 3556, 45).

Атака, описана Бернштейном [4], має виконати $c^{(1/2)n/\log_2 n}$ ітерацій алгоритму Гровера, а кожне застосування алгоритму Гровера потребує $O(n^3)$ операцій з кубітами, так кожна ітерація займає $n^{o(1)}$ на квантовому комп'ютері з розміром регістра $n^{o(1)}$. Складність квантової атаки криптосистеми на базі кодів з характеристиками (4096, 3556, 45) вимагає 2^{68} ітерацій, а кожна ітерація 2^{36} кубітових операцій, отже складність атаки приблизно 2^{100} , а це не є достатнім для 128-бітного рівня стійкості.

Інший клас криптосистем, що можуть використовуватися у постквантовому світі — це криптосистеми, які засновані на проблемі розв'язання багатовимірних квадратних рівнянь (MQ-проблема) над кінцевими полями. Розв'язання MQ рівнянь, як відомо, є NP-складною задачею і різні схеми MQ намагаються наблизитися до загального випадку. Сьогодні були запропоновані схеми підпису та шифрування, засновані на проблемі вирішення багатовимірних квадратних рівнянь, але тільки схеми підпису є стійкими до криптоаналізу.

На такий клас криптосистем запропоновано такі атаки, як пряма атака, атака погодження, атака Кіпніс-Шаміра. Проте всі ці атаки мають субекспоненційну чи експоненційну складність, квантових атак на такий клас криптосистем ще не було запропоновано, тому що алгоритм Шора чи алгоритм Гровера не підходять для реалізації квантової версії наведених вище класичних атак [3].

Криптографія, яка заснована на ізогінеї становить цікаву альтернативу наведеним вище напрямкам постквантової криптографії [6]. Це пояснюється тим, що вона базується на природній обчислювальній проблемі теорії чисел, а саме на проблемі обрахунку ізогінезису між еліптичними кривими. Ці системи можна віднести до одного з напрямків постквантової криптографії, такі системи базуються на теоретико-числовому припущенні. Враховуючи те, що національний стандарт вироблення та перевірки цифрового підпису базується на еліптичних кривих, то такий напрямок є надзвичайно важливим і перспективним для використання в Україні.

В роботі [6] наведено аналітичні показники стійкості такої криптосистеми, де показано, що складність криптоаналізу такої криптосистеми з використанням класичних комп'ютерів складає:

$$O(\sqrt[4]{p}), \quad (12)$$

для квантових комп'ютерів:

$$O(\sqrt[6]{p}). \quad (13)$$

Порівняльний аналіз квантового та класичного криптоаналізу криптосистем на базі ізогінеї еліптичних кривих в табл. 4.

Таблиця 4

Порівняльний аналіз стійкості на базі ізогінеї еліптичних кривих проти класичного та квантового криптоаналізу

Розмір поля $GF(p)$, біт	512	768	1024	2048
Класична атака, бітових операцій	$3 \cdot 10^{38}$	$6 \cdot 10^{57}$	10^{77}	10^{154}
Квантова атака, квантових гейтів	$5 \cdot 10^{25}$	$3 \cdot 10^{38}$	$2 \cdot 10^{51}$	$5 \cdot 10^{102}$

Отже криптосистеми на базі ізогінеї еліптичних кривих мають велику стійкість як проти квантового, так і проти класичного криптоаналізу, при цьому розміри поля мають невеликі розміри.

Якщо стисло охарактеризувати постквантові криптосистеми, то криптосистеми на базі решіток, на сьогодні, призначені більше для шифрування інформації, так схеми вироблення цифрових підписів на основі решіток є менш розвинуті, ніж схеми шифрування. Водночас криптосистеми на базі геш-функцій та мультиваріативні поліноми більш готові, на сьогодні, для вироблення цифрових підписів, ніж для шифрування інформації. Криптосистеми на базі ізогінеї зараз більше пов'язані з шифруванням та з протоколом автентифікації. Класично протоколи автентифікації суб'єкта пов'язується зі схемою Фіат-Шаміра, проте така схема є уразливою до можливостей квантового криптоаналізу. Нещодавно було запропоновано схему на основі ізогінезису еліптичних кривих, яка пропонує схему виготовлення та перевірки цифрового підпису, автентифікації та може бути застосована у постквантовому світі [6]. Сьогодні важко побуду-

вати схеми цифрового підпису, які будуть стійкими до квантового криптоаналізу, єдина відома незаперечна схема підпису, що була запропонована, заснована на лінійних кодах.

Порівняння класів постквантових криптосистем (крім симетричних шифрів) наводиться у табл. 5.

ВИСНОВКИ

У статті наведено наші оцінки стійкості сучасних популярних асиметричних криптосистем на основі таких математичних проблем як складність факторизації цілого числа та вирішення дискретного логарифмічного рівняння (в полі та у групі точок еліптичної кривої) проти класичного та квантового криптоаналізу. Оцінки показують, що з використанням алгоритму Шора такі криптосистеми як RSA, DSA, ECC та подібні до них будуть скомпрометовані з використанням поліноміального числа квантових гейтів.

Хоча стійкість асиметричних криптосистем є поліноміальною і збільшення розмірів загальносистемних параметрів не дає суттєвого підвищення стійкості проти квантового криптоаналізу, проте для його проведення квантовий комп'ютер повинен мати доволі велику, на сьогодні момент, кількість кубітів, саме на цьому може ґрунтуватися певний час стійкість таких криптосистем. Розміри загальносистемних параметрів криптосистеми на базі еліптичних кривих можна підняти аж до 1024 біт, тоді квантовий комп'ютер повинен мати 7218-кубітний процесор для зламу такої криптосистеми.

У статті проведено аналіз постквантових криптосистем, які можуть застосовуватися у випадку появи квантових комп'ютерів, що можуть реалізувати квантові алгоритми Шора та Гровера. Проведений аналіз таких криптосистем показав, що з використанням алгоритму Гровера можна значно зменшити складність атаки на симетричні криптосистеми (блокові шифри та геш-функції), криптосистеми на базі решіток (NTRU), криптосистеми на базі геш-функцій, кодів та ізогінеї еліптичних кривих, проте такий криптоаналіз потребує субекспоненційної кількості квантових гейтів.

Література

- [1] Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor // SIAM J. Comput. — 1997. — 26 (5). — P. 1484–1509.
- [2] Grover, L. K. A fast quantum mechanics algorithm for database search / L. K. Grover. // — Proceeding of the 28th ACM Symposium on Theory of Computation, New York: ACM Press. — 1996. — P. 212–219.
- [3] Bernstein, D. Post-quantum cryptography / D. Bernstein, J. Buchmann, E. Dahmen. — Berlin: Springer, 2009. — 246 p.
- [4] Bernstein, D. Grover vs. McEliece. Pages / D. Bernstein // Proceedings of PQCrypto 2010, Post-quantum cryptography: third international workshop proceeding. — Springer. — 2010. — P. 73–80.
- [5] Stefan Heyse. Post quantum cryptography: implementing alternative public key schemes on embedded devices : dissertation for the degree of doktor-ingenieur : 10.2013 / Stefan Heyse. — Bochum, 2013. — 235 p. — Bibliogr. : P. 205–223.
- [6] De Feo, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies / L. De Feo, D. Jao, J. Plut // PQCrypto. — 2011. — 24 p.
- [7] Горбенко, Ю.І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю.І. Горбенко, Р.С. Ганзя // Харків: «Восточно-Европейский журнал передових технологій». — 2014. — Том 6. № 1 (67). — 8–15 с.
- [8] Горбенко Ю.І. Аналіз стійкості популярних криптосистем проти квантового криптоаналізу на основі алгоритму Гровера / Ю.І. Горбенко, Р.С. Ганзя // Київ: Захист інформації: Науково-практичний журнал, 2014. — Том 16, № 2. — С. 106–112.

Надійшла до редколегії 17.06.2014

Горбенко Юрій Іванович, фото та відомості про автора див. на стор. 251.



Ганзя Роман Сергійович, випускник кафедри безпеки інформаційних технологій ХНУРЕ. Наукові інтереси: дослідження стійкості асиметричних криптосистем.

Таблиця 5

Порівняння постквантових криптосистем

Клас криптосистеми	Вироблення / перевірка підпису	Шифрування / розшифрування	Розмір ключа	Тип даних	Основні операції
На основі решіток: NTRU загальні решітки	Можливо Можливо	Так Так	<0,1 кБ ≈100 кБ	Zq GF(2m)	Згортання Множення матриць
Мультиваріативні поліноми	Так	Ні	≈10 кБ	GF(2m)	Множення матриць, рішення лінійної системи рівнянь
На основі геш-функцій	Так	Ні	≈20 Б	Вихід геш-функції	Гешування
На основі кодів	Потребує багато обчислень	Так	≈100 кБ	GF(2m)	Множення матриць, декодування
Ізогінезис супер-сингулярних еліптичних кривих	Так	Ні (присутній протокол встановлення ключів)	<1 кБ	GF(p)	Операції на еліптичній кривій

УДК 004.056

Анализ стойкости постквантовых криптосистем
/ Ю.И.Горбенко, Р.С. Ганзя // Прикладная радио-
электроника: научн.-техн. журнал. — 2014. — Том 13. —
№ 3. — С. 268—274.

В работе приводятся оценки стойкости популяр-
ных асимметричных криптосистем против квантового
криптоанализа на основе алгоритма Шора, показаны
основные классы криптосистем, которые будут стой-
кими к квантовому криптоанализу на основе алгорит-
мов Шора и Гровера. Приводятся оценки стойкости
постквантовых криптосистем против классического и
квантового криптоанализа.

Ключевые слова: постквантовая криптография, ал-
горитм Шора, алгоритм Гровера, NTRU.

Табл.: 5. Библиогр.: 10 назв.

UDC 004.056

Analyzing resistance of postquantum cryptosystems /
Yu.I. Gorbenko, R.S. Hanzia // Applied Radio Electro-
nics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 268—274.

This paper presents estimations of resistance of popu-
lar asymmetric cryptosystems against quantum cryptanaly-
sis based on Shor's algorithm, the basic classes of cryptosys-
tems are shown that are resistant to quantum cryptanalysis
on the bases of Shor's and Grover's algorithms. Estimations
of resistance of postquantum cryptosystems against classical
and quantum cryptanalyses are provided.

Keywords: postquantum cryptography, Shor's algo-
rithm, Grover's algorithm, NTRU.

Tab.: 05. Ref.: 10 items.

STORK – ПЕРСПЕКТИВНЫЙ ПРОЕКТ ЕВРОПЕЙСКОЙ ТРАНСНАЦИОНАЛЬНОЙ ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ

Ю.В. ГОНЧАРОВА, А.А. ЕРЁМЕНКО

Анализируются основные проблемные вопросы и результаты текущей стадии проекта STORK 2.0 ЕС, в части обеспечения трансграничной идентификации физических и юридических лиц, выполняемого в ходе реализации Регламента Европейского парламента и Совета по электронной идентификации и доверительным (трастовым) услугам для электронных операций на внутреннем рынке ЕС. Обсуждаются возможности Украины, как участника проекта, а также альтернативные методы решения задачи межграничной электронной идентификации.

Ключевые слова: STORK, электронная идентификация, европейская идентификация, трансграничные сервисы, электронные доверительные услуги.

ВВЕДЕНИЕ

В информационном пространстве технологически развитых государств и союзов интенсивно решаются проблемы предоставления физическим и юридическим лицам широкого выбора инструментов, облегчающих ведение онлайн бизнеса, электронного документооборота и электронных государственных сервисов и др., без пространственных и временных ограничений. Важные результаты в этом направлении получены в ЕС. Украина как государство, которое движется к европейской интеграции, имеет возможность использовать и принимать участие в разработке и внедрении перспективных электронных сервисов самых удачных мировых решений. Однако, в последние годы в ЕС, в этом направлении выявлено ряд проблем и возникших противоречий. На их основе сделан вывод о необходимости расширения электронных услуг, сделать их в пределах ЕС трансграничными. Основные задачи разрешения указанных противоречий представлены и утверждены в Регламентах ЕС 2012 и 2014 года [1, 2]. При этом, на первом этапе создания единого цифрового рынка в ЕС, необходимо решить задачи безопасной электронной идентификации и аутентификации юридических и физических лиц.

На предложение Европейского парламента и Совета 3 апреля 2014 года принят Регламент «Об электронной идентификации и доверительных услугах для электронных операций на внутреннем рынке» [2]. В Регламенте изложены требования и задачи обеспечения безопасных электронных услуг между предприятиями, гражданами и государственными органами с сохранением целостности данных. Это позволит повышать эффективность государственных и частных онлайн-услуг, электронного бизнеса и электронной торговли в ЕС. Введено понятие доверительной услуги, т. е. услуги, входящая в состав создания, проверки, подтверждения правильности, обработки и хранения электронных подписей, электронных печатей, электронных меток времени, электронных документов, услуг электронной до-

ставки, подтверждения подлинности веб-сайтов и электронных сертификатов.

Впоследствии была принята методология прагматичного внедрения вышеназванных механизмов, для реализации чего был начат ряд проектов, одним из которых является проект реализации электронной идентификации STORK[3]. На сегодняшний день актуальной является версия STORK 2.0 (*Secure identity across borders linked 2.0 – Безопасная трансграничная идентификация 2.0*) [4]. Она представляет собой трехлетний проект (2012–2015 годы), целью которого является создание и внедрение единой общеевропейской системы электронной идентификации. Проект анонсировал 19 партнеров из 11 стран, однако впоследствии число партнеров увеличилось до 58.

Проект STORK 2.0 призван повысить эффективность сотрудничества государственного и частного секторов на национальном и общеевропейском уровнях, упростить административные формальности, предоставляя упрощенный онлайн доступ к публичным трансграничным услугам через границы Европейского союза (далее – ЕС) в защищенной, конфиденциальной, а, следовательно, безопасной среде.

При реализации проекта STORK 2.0 появится возможность взаимодействия с национальными идентификаторами, позволяя использовать их в любом государстве-члене ЕС без ограничений, посредством связи с национальными системами идентификации.

Считается, что реализация проекта также увеличит интероперабельность электронной идентификации в рамках границ европейских государств, а также обеспечит электронную аутентификацию физических лиц с полномочиями, позволяющими представлять юридических лиц. Возможности использования электронной идентификации в Европе показаны на рис 1.

Целью настоящей статьи является изложение результатов анализа проекта STORK 2.0 и предложений по их возможному использованию в Украине.



Рис 1. Использование сервисов ЕС с помощью электронной идентификации

1. ЗАДАЧИ, РЕШАЕМЫЕ В ПРОЕКТЕ STORK 2.0

1. Использование опыта предыдущих пилотных проектов STORK для внедрения четырех трансграничных проектов, а также продолжение развития предыдущих направлений.
2. Способствование достижению целей и поддержке инноваций в Европе с помощью информационно-телекоммуникационных технологий.
3. Активизация Единого рынка для государственных и коммерческих услуг, содействие мобильности внутри ЕС.
4. Расширение возможностей предпринимателей и граждан с помощью бесплатных трансграничных моделей электронного управления.
5. Обеспечение разработки общеевропейской инфраструктуры для электронной идентификации граждан и бизнес-сферы.

2. ВЫПОЛНЕННЫЕ РАБОТЫ И ДОСТИГНУТЫЕ РЕЗУЛЬТАТЫ

На сегодняшний день в рамках проекта реализованы следующие задачи:

- Проведён обзор и подробный анализ существующих инфраструктур электронной идентификации в каждой стране-члене ЕС, принимающей участие в STORK 2.0: определены поддерживаемые услуги и процедуры каждого государства относительно аутентификации, авторизации и роли полномочий.
- Сделан анализ правовых норм, включая ключевые понятия, процедуру возложения полномочий на представление физическими лицами юридических лиц (форма, содержание и нотариальное участие), обязательства проверки получателем полномочий, правовые ограничения, срок действия и аннулирование полномочий, а также возложение полномочий с использованием электронных средств (в том числе необходимость ЭЦП).
- Кроме того, STORK 2.0 выявил проблемные вопросы защиты данных: проблемы, которые включают, в частности, роль внешних поставщиков атрибутов, обработку личных данных (в частности, данных о состоянии здоровья, бан-

ковских данных), и передачу персональных данных службе провайдера в странах, где правила защиты данных ЕС не применяются (в частности, в Турции).

• Наконец, одним из основных итогов STORK была QAA модель (Quality Authentication Assurance — обеспечение качественной аутентификации), что способствовало достижению допустимых уровней качества для различных решений электронной идентификации. Оригинальный фреймворк STORK QAA включает четыре уровня обеспечения аутентификации и позволяет быстро сопоставлять электронные идентификаторы, предоставляя возможность поставщикам услуг выбрать наиболее подходящий уровень гарантии для их применения.

3. ПРАВОВЫЕ ОСОБЕННОСТИ

В рамках проекта, основные юридические риски анализируются для каждой категории заинтересованных сторон, в том числе в вопросах разрешения споров, защиты данных, ответственности, гарантий уровня обслуживания, предоставлений полномочий и проблем в каждом конкретном случае (например, правила передачи персональных данных за пределами ЕС и европейской экономической зоны). Эти правовые особенности затем сопоставляются с существующей правовой базой (в основном, национальными директивами ЭЦП и Регламентом Парламента ЕС по электронной идентификации и доверительным (трастовым) услугам). Некоторые правовые проблемы, стоящие перед заинтересованными сторонами, не затронуты предлагаемым подходом (например, не рассматривается, как поставщики услуг должны соблюдать законы о защите данных), но эти вопросы и не подлежат решению в рамках проекта STORK.

Следует отметить, что это договорной подход, необходимый, прежде всего, в качестве временного (до момента принятия общих для всех стран правил электронной идентификации и доверительных услуг). Однако не исключено, что реализация данного проекта будет актуальной и после, решая, в таком случае, задачи, не решенные в предыдущих двух версиях.

Ответ на вопрос, связанный с национальным законодательством относительно полномочий, должен быть найден в национальном законодательном органе каждой из стран-участниц, на основе фактических данных в каждом конкретном случае. Применяемое законодательство установит формат и существенные требования, которым должны соответствовать полномочия.

Вопрос трансграничного использования полномочий означает, что полномочия, предоставленные лицу в стране А, должны иметь силу и применяться в стране В. Другими словами, страна В должна признавать формат и действительность полномочий, предоставленных в стране А. Это происходит в случае, если страна

В имеет правовую основу, которая предусматривает признание законов страны А, или если обе страны А и В связаны международным договором или законодательством ЕС, которые декларируют, как и в каких ситуациях принимаются иностранные полномочия.

Для юридических лиц – субъектов электронной идентификации основной задачей будет интеграция коммерческих регистров в качестве поставщиков атрибутов таким образом, чтобы физические лица, которые идентифицируются с помощью STORK, были надежно связаны с юридическим лицом. Проверка того, являются ли они компетентными в вопросах представительства юридического лица для конкретной предполагаемой операции, может быть сделана путем:

1. Формализации часто используемых полномочий. Хотя это не может быть всеобъемлющим решением и не охватит все национальные правила, варианты и исключения, такой подход должен предоставить подходящее упрощение правовой действительности.

2. Запроса совпадения этого формализованного представления с реальными взаимоотношениями физического лица-представителя и юридического лица, а также запрос подтверждения таких взаимоотношений.

4. ОСОБЕННОСТИ РЕАЛИЗАЦИИ

Основным отличием платформы STORK является возможность идентификации юридических лиц: юридический статус таких субъектов

предусматривает наличие физических лиц, способных распоряжаться от имени юридических лиц.

Процесс авторизации в таких случаях планируется реализовать следующим образом [4–6]: пользователю сперва предлагается выбрать, резидентом какой страны он является: он перенаправляется для взаимодействия с сервисами выбранного государства, предъявляет идентификационные данные, требующиеся конкретным государством (этот шаг и обеспечивает интероперабельность процедуры, поскольку вопрос идентификации на данном этапе реализован различными методами в государствах-членах ЕС, что сводит на нет возможность единой системы идентификации). Здесь пользователю предоставляется выбор, отсылать или нет свои идентификационные данные. Примечательно, что пользователь на любом этапе может отказаться от пересылки данных, что будет рассматриваться как отказ от идентификации и прерывание процедуры. При удачной верификации пользователю предоставляется возможность выбора страны, в которой расположена компания, которую он представляет: если это другая страна (не та, что была первоначально выбрана), запрашивается подтверждение на отправку идентификационных данных повторно, но уже сервисам второго государства. После этого авторизация происходит в сервисах страны, где зарегистрированы полномочия пользователя с предварительным подтверждением им своего согласия отправки идентификационных данных третьей стороне.

Алгоритм этого процесса изображен на рис. 2.

Идентификационные данные отправляются другим государствам в виде подписанного сообщения. При чем, изначально сообщение получает провайдер сервиса (service provider, SP), который перенаправляет сообщение пан-

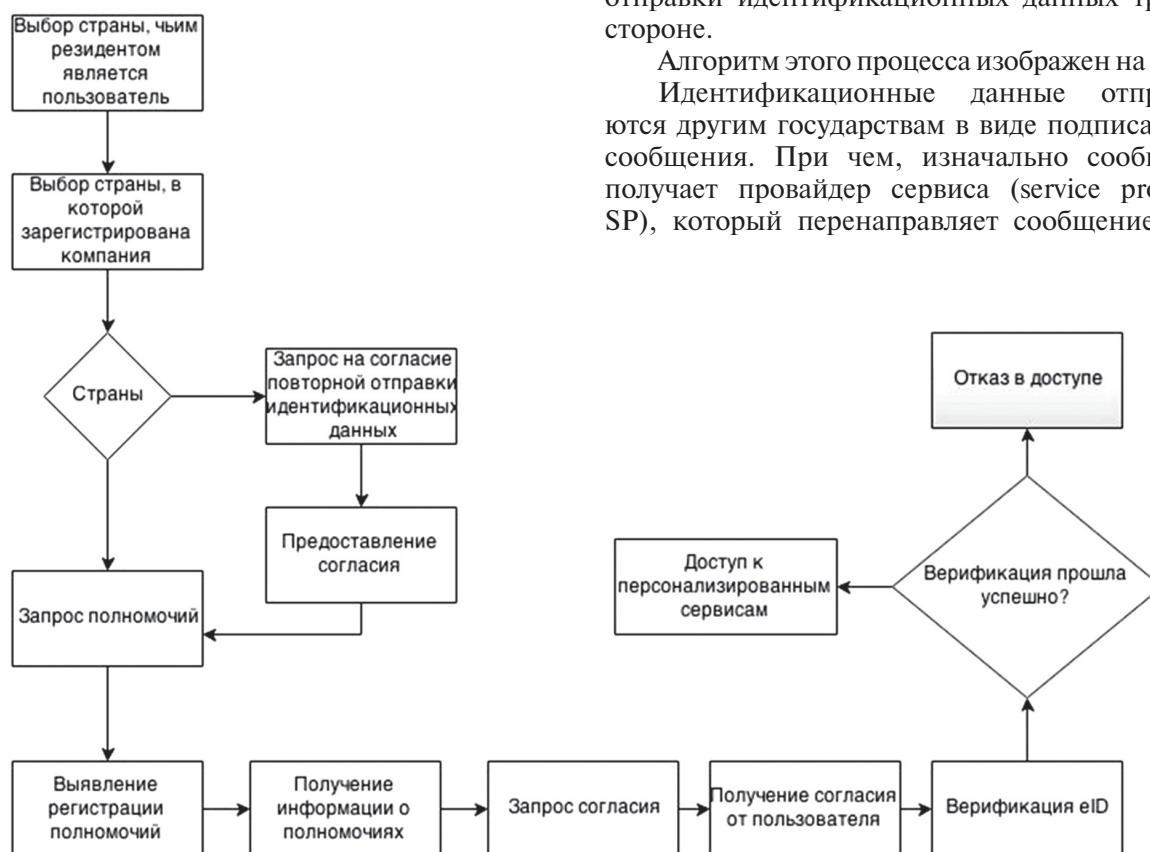


Рис. 2. Блок-схема механизма авторизации согласно платформе STORK

европейскому прокси-серверу (pan-European proxy server, PEPS), который и проверяет валидность данных, и возвращает PS набор данных, позволяющий определить полномочия того, кто подписал сообщение (см. рис. 3).

Предполагается, что внедрение подобной платформы даст толчок к развитию наиболее популярных отраслей межграничного взаимодействия.

Изначально проект STORK представил 5 пилотных проектов:

1. SaferChat (безопасный чат) демонстрирует возможность более безопасного применения чата в трансграничном контексте.

2. Student Mobility (студенческая мобильность) обеспечивает иностранным студентам доступ к online административным и академическим услугам европейских университетов.

3. eDelivery (электронная доставка) демонстрирует совместимость электронных инфраструктур доставки. Фреймворк электронной доставки позволяет государственным структурам отправлять документы гражданам через государственные границы с помощью национальных порталов электронной доставки.

4. Change of Address (смена адреса) – этот пилотный проект развивает основу для интероперабельной службы, позволяющей иностранным гражданам (с использованием электронной идентификации) уведомить все соответствующие органы об изменении адреса. Это достигается без изменения существующих процедур в каждом государстве-члене.

5. ECAS integration (European Commission Authentication Service, интеграция сервисов европейской службы аутентификации).

STORK 2.0 реализует четыре пилотные услуги, ориентированные на следующие стратегические области:

eBanking. Основная идея заключается в предоставлении возможности физическим и юридическим лицам безгранично пользоваться услугами иностранных банков через их web-сервисы (открывать банковские счета, производить финансовые операции). Ключевым моментом здесь является взаимодействие банковской и пользовательской сфер без создания дополнительных правовых и бизнес-ограничений. Проект позволит повысить безопасность и эффективность операции с электронными счетами через границы надежным образом в соответствии с Европейской директивой 2010/45/EU. Это не только повысит эффективность взаимодействия банка с клиентами, но и позволит клиентам, имеющим деловые отношения с несколькими банками, не запоминать множество идентификационных данных (таких как PIN коды), а использовать свою цифровую подпись для аутентификации.

eHealth. Данный сервис не только позволит врачам получать доступ к информации о пациенте, хранящейся на стороне страны пациента, но и самому пациенту получать данные о своей учетной записи. Основной бизнес-целью разработчики отмечают уменьшение стоимости и повышение качества услуг здравоохранения за

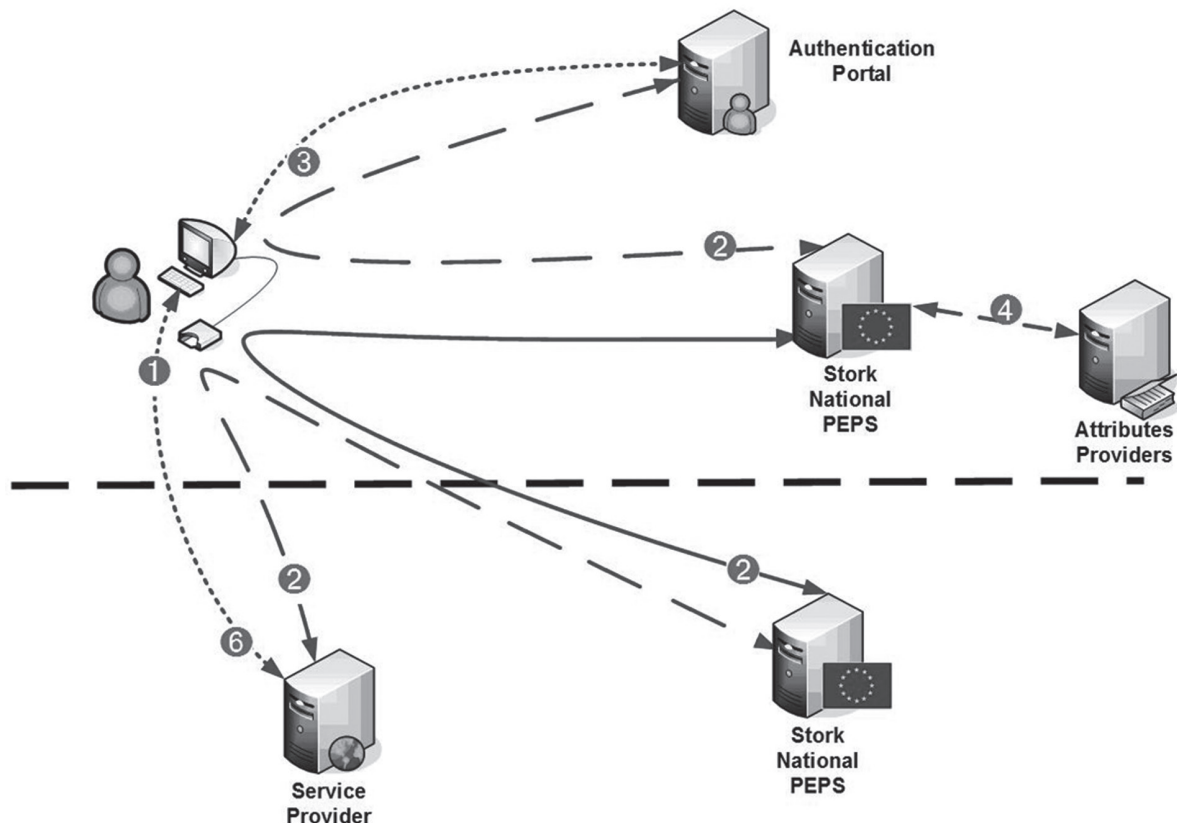


Рис. 3. Структура коммуникаций

счет привлечения информационных технологий. Действительно, данный сервис значительно облегчит взаимодействие врачей стран-членов ЕС, т. к., например, в случае имплементации данного сервиса пользователю не нужно будет производить никаких действий по сбору всей необходимой информации для иностранного врача при переводе на лечение в другую страну.

eLearning. Основной целью является построение сервисов на основе анонсируемой платформы, позволяющих гражданам, компаниям и государственным структурам взаимодействовать между собой. Конкретные цели проекта можно резюмировать следующим образом:

1. Построить трансграничные академические услуги, основанные на обмене атрибутов, удостоверяющих личность (для электронного обучения и опросов общественного мнения).

2. Облегчить использование академической информации пользователями, государственными и частными организациями.

3. Показана возможность интеграции других существующих услуг относительно проверки сертификатов, необходимых в учебных курсах от других, чем источников.

С точки зрения бизнеса, цели проекта будут способствовать изучению возможности разработки, настройки и организации высшего образования системы электронного обучения для выхода за пределы национальных границ и способствованию созданию Европейской зоны высшего образования (European Higher Education Area. ENEA); принятию со стороны академического сообщества, развитию ключевого набора действия, которые могут сильно способствовать распространению и будущему использованию электронных учетных данных; привлечению частного сектора в использовании академической информации, предоставляя её средства в своих целях; доказательству требуемой квалификации и спецификации, которые будут осуществляться на сайте, как это предписано директивой службы.

eGovernment for Business. Существуют два варианта использования данного сервиса: «Зачисление в публичные регистры» и «One-stop shop» сервис (Единый разрешительный центр – рабочий орган соответствующего городского совета или районной/областной администрации, в котором представители местных разрешительных органов и государственный администратор действуют по принципу организационного единства по выдаче документов разрешительного характера, переоформления, выдачи дубликатов, аннулирования документов разрешительного характера). Зачисление в публичные регистры относится к общественным, административным услугам, которые являются частью требований к предприятиям, желающим работать в конкретных экономических секторах или областях.

5. АНАЛИЗ ВОЗМОЖНОСТИ УЧАСТИЯ УКРАИНЫ В ПРОЕКТЕ

На сегодняшний день можно говорить о хорошо развитой инфраструктуре электронной цифровой подписи в Украине: на базе PKI (public key interface) развёрнута широкомасштабная организационно-техническая структура, предназначенная для предоставления услуг ЭЦП, объединяющая центры сертификации ключей, контролирующий орган, пользователей в единую систему. Учитывая предпочтительное использование именно PKI в ЕС, необходимо отметить, что в нашей стране созданы все технические условия для внедрения системы единой идентификации физических и юридических лиц с помощью усиленного сертификата открытого ключа.

С точки зрения правового регулирования, на сегодняшний день активно разрабатывается нормативно-правовая база, способствующая развитию электронных доверительных услуг в Украине согласно проекту Регламента Европейского Парламента и Совета по электронной идентификации и доверительных (трастовых) сервисах для электронных операций на внутреннем рынке. Касательно возможности представительства других лиц, текущий проект Закона Украины «Про электронную цифровую подпись» в ст. 3 устанавливает следующее требование: «ЭЦП по статусу приравнивается к собственноручной подписи в случае, если ЭЦП наложена непосредственно подписантом – физическим лицом или уполномоченным представителем юридического лица» и «Электронная цифровая подпись по правовому статусу приравнивается к штампу юридического лица или физического лица – предпринимателя».

Именно это необходимое условие правового статуса ЭЦП обеспечивает корректное правовое взаимодействие бизнес-партнеров (юридических лиц) из Украины в рамках ЕС через их представительство физическими лицами. Использование собственноручной подписи или печати на бумажном документе предполагает их проставления непосредственно подписантом или лицом, уполномоченным на использование печати в делопроизводстве. Поэтому, для обеспечения признания ЭЦП аналогом собственноручной подписи или печати по всем нормам, в том числе международным, предусмотрено непосредственное владение личным ключом подписанта и хранение его в тайне.

ВЫВОДЫ

Таким образом, в связи с трансграничным характером информационных отношений в глобальной информационной сфере, возникает необходимость их упорядочения путем избрания на глобальном уровне единых нормативно-правовых подходов для применения совместных согласованных мер. Достижение этих целей осуществляется, среди прочего, путем международного сотрудничества и принятия международно-пра-

вовых актов с учетом имеющегося опыта регулирования трансграничных информационных отношений, приобретенного на протяжении истории развития современного международного права.

Исходя из вышеизложенного, логичным является вывод, что в момент принятия обновленной нормативно-правовой базы Украина может стать достойным претендентом на участие в выполнении проекта. При этом дальнейшая Евроинтеграция сулит Украине относительно безболезненное наследование принципов и механизмов, принятых в ЕС, которые относятся к электронной идентификации.

Литература

- [1] Brussels, XXX. COM(2012) 238/2. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) {SWD(2012) 135} {SWD(2012) 136}. 32. http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision
- [2] Регламент (ЕС) № ... / 2014 Европейского Парламента и Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій а внутрішньому ринку (1) (COM (2012) 0238 - C7-0133/2012 - 2012 / 0146 (COD))
- [3] STORK project. [Электронный ресурс]. Режим доступа: <https://www.eid-stork.eu/> Дата обращения: 09.06.2014.
- [4] STORK 2.0 project. [Электронный ресурс]. Режим доступа: <https://www.eid-stork2.eu/> Дата обращения: 09.06.2014.
- [5] Commission welcomes political agreement on new EU regulation for electronic ID and trust services. European Commission - MEMO/14/151 28/02/2014 [Электронный ресурс]. Режим доступа: http://europa.eu/rapid/press-release_MEMO-14-151_en.htm Дата обращения: 09.06.2014
- [6] FutureID - Shaping the Future of Electronic Identity. 2014 [Электронный ресурс]. Режим доступа: <http://www.futureeid.eu/>

Поступила в редколлегию 18.06.2014

Гончарова Юлия Владимировна, студентка Харьковского национального университета имени В.Н. Каразина, факультет компьютерных наук, юридический факультет. Научные интересы: информационное право, правовое регулирование информационной безопасности.



Еременко Алина Александровна, экономист, ответственная за ведение кадрового делопроизводства в АО «Институт информационных технологий». Научные интересы: кадровая безопасность, методы и средства защиты информации.

УДК 34: 002: 681.5.015

STORK — перспективный проект европейской транснациональной электронной идентификации / Ю.В. Гончарова, А.О. Ерьоменко // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 275–280.

Аналізуються основні проблемні питання та результати поточної стадії проекту STORK 2.0 ЄС, в частині забезпечення транскордонної ідентифікації фізичних та юридичних осіб, виконуваного в ході реалізації Регламенту Європейського парламенту і Ради з електронної ідентифікації і довірчих (трастових) послуг для електронних операцій на внутрішньому ринку ЄС. Обговорюються можливості України, як учасника проекту, а також альтернативні методи розв'язання задачі міжкордонної електронної ідентифікації.

Ключові слова: STORK, електронна ідентифікація, європейська ідентифікація, транснаціональні сервіси, електронні довірчі послуги.

Л.: 3. Бібліогр.: 6 найм.

UDC 34: 002: 681.5.015

STORK — promising project of European transnational electronic identification / Yu.V. Goncharova, A.A. Yeriomenko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 275–280.

The paper analyzes the major issues and the results of the current phase of the project STORK 2.0 EU in terms of ensuring transborder identification of individuals and juridical persons, which is performed during the implementation of the Regulations of the European Parliament and the Council for electronic identification and confidence (trust) services for electronic transactions in the EU internal market. The possibilities of Ukraine as a participant in the project, as well as alternative methods of solving the problem of cross-border e-identification are discussed.

Keywords: STORK, electronic identification, European identification, transnational services, electronic trust services.

Fig.: 3. Ref.: 6 items.

ВЛИЯНИЕ СВОЙСТВ СОВРЕМЕННЫХ ПРОЦЕССОРОВ НА ПРОИЗВОДИТЕЛЬНОСТЬ ПРОГРАММ

Е.Г. КАЧКО, Д.С. БАЛАГУРА, К.А. ПОГРЕБНЯК

Проводится анализ и сравнение способов оптимизации производительности программ. Приводятся теоретические и экспериментальные результаты исследований влияния на производительность конвейерной обработки, кеш памяти и распараллеливания вычислений. Дается оценка эффективности использования разных технологий для повышения производительности и рекомендации по их применению.

Ключевые слова: конвейер, кеш-память, криптографические преобразования, параллельные вычисления, TBB, OpenMP.

ВВЕДЕНИЕ

На программы для криптографических преобразований очень часто накладываются жесткие ограничения на временные и пространственные характеристики. Эти требования связаны с масштабом использования этих преобразований и техническими ограничениями. В данной работе рассматриваются методы уменьшения временной сложности программ.

При оценке вычислительной сложности программ обычно учитывается количество операций, которые надо выполнить. Если алгоритм требует меньшее количество операций или одинаковое количество, но более простых операций, он считается более эффективным. Такой критерий оценки был справедлив для скалярных процессоров без конвейеров и других технических решений для увеличения быстродействия.

В работе рассмотрено влияние конвейера, кеша и параллелизма на временные характеристики программ. В конце показан учет приведенных факторов на примере оптимизации кода для умножения полиномов для алгоритма NTRU.

1. ИСПОЛЬЗОВАНИЕ КОНВЕЙЕРА

Для архитектуры X86 (i486) в 1989 году был добавлен простейший конвейер, содержащий 5 стадий: выборка команды, ее декодирование (определение кода и операндов), определение базы и смещения для адреса из операнда (только один операнд мог быть адресом памяти), выполнение инструкции, и, наконец, запись результата в регистр или память. Использование конвейера позволяет существенно уменьшить время выполнения последовательности команд. Действительно, пусть надо выполнить n команд. Пусть время выполнения каждой команды без конвейера равно 1. Тогда для выполнения этих команд потребуется $T_1 = n$ единиц времени. Пусть эта же последовательность команд выполняется с помощью конвейера, содержащего m блоков. В идеале каждый блок будет выполнять свою операцию за $1/m$ единиц времени (накладными расходами, связанными с использованием конвейера, пренебрегаем). Тогда время выпол-

нения n команд равно $T_2 = 1 + n/m$ единиц времени. При большом n получаем ускорение приблизительно в m раз. Вот почему современные процессоры содержат не менее 10 блоков конвейера, а иногда и больше 20 [1]. Нарастивание числа блоков конвейера ограничено только технологическими возможностями. Конвейер наиболее эффективен, если в программе нет инструкций перехода, которые нарушают естественный порядок выполнения команд. Инструкции перехода, нарушающие этот порядок, приводят к необходимости останова конвейера, связанного с необходимостью обработки другой последовательности команд, или встраиванию дублирующей ветви (так называемого спекулятивного выполнения), когда фактически выполняются команды для нескольких ветвей и «правильная» ветвь определяется после завершения выполнения команды перехода. Понятно, что оба решения приводят к потерям. Причем, эти потери тем существенней, чем больше команд перехода в программе. Заметим, что использование блоков прогнозирования переходов, которые являются составной частью всех современных процессоров, позволяют уменьшить эти потери только в случае успешного прогнозирования, которое гарантировано только в случае, если направление перехода не является случайным. Рассмотрим несколько примеров, которые позволят определить количественно потери, связанные с использованием команд перехода.

Пример 1. Пусть необходимо определить количество отрицательных чисел последовательности. Очевидно, что для подсчета можно использовать код¹

```
int count = 0;
for (int i = 0; i < n; ++i){
    if (src[i] < 0)
        count++;
}
```

¹ Для задания кода используется синтаксис языка C. Процессор Intel (R) Core (TM) i5 – 4440 CPU @ 3.10 GHz

Определим количество необходимых операций для различных вариантов исходных данных (все числа не отрицательные, все числа отрицательные, отрицательные и неотрицательные числа равновероятны). При определении этого количества операции, связанные с организацией цикла, не учитываются, т. к. они необходимы для всех вариантов исходных данных.

1. Если все числа не отрицательные, то требуется n операций сравнения.

2. Если все числа отрицательные, то требуется n операций сравнения и n операций увеличения на 1 счетчика чисел.

3. Если отрицательные и неотрицательные числа равновероятны, то требуется n операций сравнения и $n/2$ операций увеличения на 1 счетчика чисел.

Таким образом, наибольшее количество операций требуется в случае, когда все числа отрицательные. Результаты вычислительного эксперимента приведены в табл. 1. При задании числа операций не учитываются команды сравнения, количество которых одинаково для всех вариантов.

Таблица 1

Определение количества отрицательных чисел ($n = 1024 * 1024$)

	1	2	3
Количество операций	0	n	$n/2$
Время выполнения (мс)	0.47	0.37	4.3

Как следует из табл. 1, ожидания не подтвердились, вариант, который ожидался как самый быстрый, только на втором месте (уступает второму варианту 27%). Вариант 3, который должен быть на втором месте, оказался последним и требует более чем в 11 раз больше времени, чем второй, по прогнозам, самый медленный вариант. Такой результат связан с потерями в конвейере, которые пропорциональны количеству ошибок прогнозирования. Этих ошибок совсем нет для 1 варианта, и максимальное количество для варианта 3. Для рассмотренного выше примера легко написать код без команды перехода, который основывается на внутреннем представлении положительных и отрицательных чисел.

```
int count = 0;
for (int i = 0; i < n; ++i)
    count -= src[i] >> 31;
```

Заметим, что в данном случае нет команд перехода, а на каждой итерации надо выполнить две операции. Общее время выполнения в этом случае не зависит от типа исходных данных и составляет 0.5 мс, что практически совпадает с первым вариантом.

Пример 2. Алгоритм LLL, который используется в одной из атак для криптоалгоритма NTRU[2], необходимо для заданного числа с плавающей точкой находить ближайшее целое (округлять это число). Для выполнения этой опе-

рации можно использовать код (для одной итерации):

```
dest[i] = (int)(src[i] + (src[i] < 0 ? -0.5 : 0.5));
```

Фактически в данном случае используется одна операция сравнения $src[i] < 0$ и одна операция сложения. Если предположить, что вероятность отрицательного и неотрицательного чисел одинакова, то естественный порядок будет нарушаться в половине случаев, и прогнозирование здесь не поможет. Код без команды перехода (для одной итерации):

```
double RoundConst[] = {0.5, -0.5};
```

```
...
```

```
dest[i] = (int)(src[i] + RoundConst[*(unsigned*)&src[i] + 1] >> 31]);
```

В последнем случае операции сравнения нет, но для каждой итерации используются операции вычисления адреса и разадресации, сдвига, определение элемента массива с заданным индексом, т.е. больше операций, чем в первом случае.

В табл. 2 приведены результаты для вычислительного эксперимента с использованием (Вариант 1) и без использования (Вариант 2) команды перехода

Таблица 2

Округление чисел ($n = 1024 * 1024$)

	Вариант 1	Вариант 2
Время (мс)	17	2.4

Таким образом, второй вариант позволяет получить ускорение в 7 раз, хотя требует больше операций для каждой итерации.

Примеры, приведенные выше, показывают, что наличие команд перехода существенно влияет на вычислительную сложность кода, необходимо минимизировать количество этих команд.

2. КЕШ-ПАМЯТЬ

Современные процессоры имеют частично ассоциативный кеш для хранения команд и данных. Частичная ассоциативность означает, что данные помещаются не в любое место кеша, а в место, которое определяется его адресом. Пусть размер внутреннего кеша n байтов (как правило, это 32 КБ или 64 КБ), элемент кеша содержит k байтов (k обычно равно 64), кеш m -ассоциативный, т.е. в строке кеша помещается m элементов по k байтов. Это означает, что если расстояние между адресами данных, которые используются последовательно, больше 64, для каждого данного потребуется новая операция загрузки его в кеш. Эти операции очень дорогие. А если расстояние между адресами данных, которые используются последовательно, кратно n/m , то эти данные используют только одну строку кеша. Таким образом, каждый $m+1$ элемент массива располагается в кеше вместо первого элемента, хотя весь остальной кеш может быть свободным.

Пример 3. В алгоритме LLL необходимо вычислять скалярное произведение двух векторов. В матрицах, которые используют этот метод, вектора являются векторами – столбцами. В языках высокого уровня обычно элементы матрицы располагаются по строкам.

Код для вычисления скалярного произведения:

```
double SMCol (double *b, double *bz, int k, int l, int n){
    int n2 = n * n;
    double *pbk = b + k, *pbzl = bz + l, s = 0;
    for (int i = 0; i < n2; i+=n){
        s+=pbk [i] * pbzl[i];
    }
    return s;
}
```

Здесь *b*, *bz* – матрицы, из которых используются векторы – столбцы (задаются как одномерные массивы размерностью *n*n*); *k*, *l* – номера столбцов для векторов.

В этом случае для каждого элемента вектора фактически выбирается 64 байта (8 чисел типа *double*), но используется только одно число. Так как *n* обычно большое (для NTRU минимальное значение *n* равно 802), то для формирования скалярного произведения будет 2*n* промахов кеша. Если исходные матрицы расположить так, что вектор будет строкой матрицы, то количество промахов кеша уменьшится в 8 раз. А так как промах кеша «стоит» значительно больше, чем вычисление *s+=pbk [i] * pbzl[i]*; то производительность в этом случае должна увеличиться больше, чем в 8 раз. Результаты вычислительного эксперимента приведены в табл. 3

Таблица 3

Скалярное умножение
(*n* = 1499 * 2², данные типа *double*)

	Вектор-столбец	Вектор-строка
Время (мс)	0.226	0.0033

Получаем ускорение более, чем в 68 раз.

3. ПАРАЛЛЕЛИЗМ

В современных процессорах реализован параллелизм на уровне команд, данных и потоков.

Параллелизм команд означает, что отдельные команды, если между ними нет зависимостей, выполняются параллельно. Это свойство процессора называется суперскалярностью, и обеспечивается самим процессором и компиляторами.

Параллелизм данных означает параллельную обработку блока данных. Обеспечивается за счет использования SIMD команд.

Параллельное выполнение потоков означает одновременное выполнение потоков разными ядрами процессора, обеспечивается с по-

мощью функций операционной системы для управления потоками, специальными средами для разработками параллельных программ, например, Open MP или специальными библиотеками, например, TBB.

В настоящее время наиболее применимыми из класса SIMD команд являются SSE и AVX³ SSE команды одновременно обрабатывают блок длиной 128 бит, компонентами блока могут быть числа с плавающей точкой с обычной и двойной точностью (типы данных *__m128*, *__m128d* соответственно) и целые числа длиной от 1 до 8 байтов (тип данных *__m128i*). AVX команды обрабатывают блок данных длиной 256 бит, в перспективе до 1024 бит, компонентами блока могут быть числа с плавающей точкой с обычной и двойной точностью (типы данных *__m256*, *__m256d* соответственно), целые данные длиной 1–8 байтов (тип данных *__m256i*)[1].

Пример 4. Вычисление скалярного произведения для векторов – строк. Так как количество элементов в блоке зависит от размера элемента, рассмотрим влияние типа данных на временные характеристики кода.

Код для вычисления скалярного произведения, не зависящий от типа:

```
template <typename T>
T SM (T *x, T *y, int n){
    T s = 0;
    for (int i = 0; i < n; ++i){
        s+=x[i] * y [i];
    }
    return s;
}
```

Пример кода для вычисления скалярного произведения для данных типа *float* :

```
float SSE_SM_float (float *x, float *y, int n){
    __m128 *x128 = (__m128*)x, *y128 = (__m128*)y, s128 = _mm_setzero_ps ();
    float *s = (float *)&s128;
    for (int i = 0; i < n/4; ++i)
        s128 = _mm_add_ps (_mm_mul_ps(x128 [i], y128 [i]), s128);
    return s[0] + s [1] + s[2] + s [3];
}
```

Временные характеристики кода для различных типов данных приведены в табл. 4

Таблица 4

Скалярное умножение (*n* = 1024*1024).
Использование SSE операций

	short	int	float	double
Без SSE	0.6	0.85	3.4	1.6
С SSE	0.16	0.77	0.93	1.5

Таким образом, использование SSE эффективно для всех типов данных, эффективность тем больше, чем больше элементов данного типа помещается в блоке.

³ Необходимо проверять возможность использования!

² Такое значение *n* выбрано с учетом максимальной размерности многочлена для NTRU

Наиболее простым способом перехода от последовательного к параллельному выполнению потоков является использование OpenMP[3]. Эта технология позволяет создавать один и тот же код для последовательного и параллельного выполнения, поддерживается большинством современных ОС общего назначения и языков программирования C, C++, FORTRAN.

Технология создания параллельных программ предусматривает предварительную разработку последовательного кода с максимальной эффективностью. Этот код используется в качестве меры при сравнении и в качестве источника для тестирования. Для вычислительного эксперимента будем использовать скалярное произведение без и с использованием SSE.

Пример кода для параллельного выполнения с SSE :

```
float OPENMP_SSE_SM_float_ (float *x, float
*y, int n){
    __m128 S [SM_ThreadNum];
    #pragma omp parallel for
    for (int i = 0; i < SM_ThreadNum; ++i){
        int n4 = n/4, h = n4 /SM_
ThreadNum;
        __m128 *px128 = (__m128 *)x, *py128 =
(__m128 *)y, s;
        int begin = i * h, end = begin + h;
        if (i == SM_ThreadNum - 1) end =
n4;
        s= _mm_setzero_ps();
        for (int j = begin; j < end; ++j)
            s = _mm_add_ps (s, _mm_
mul_ps (px128 [j], py128 [j]));
        S [i] = s;
    }
    for (int i = 1; i < SM_ThreadNum; ++i) S [0]
= _mm_add_ps (S[0], S [i]);
    float *s = (float *)&S [0];
    return s[0] + s [1] + s [2] + s [3];
}
```

Здесь SM_ThreadNum – количество потоков, которое определяется числом ядер процессора.

Временные характеристики параллельного кода для различных типов данных приведены в табл. 5.

Таблица 5

Скалярное умножение (n = 1024*1024).
Использование OpenMP. SM_ThreadNum] = 4

	short	Int	float	double
Лучший без OpenMP	0.16	0.77	0.93	1.5
Лучший с OpenMP	1.3	0.48	0.51	1.4

В данном случае небольшой эффект достигнут для всех типов данных кроме данных типа short. Незначительность эффекта объясняется тем, что время выполнения параллельной ветви

небольшое. В этом случае на производительность существенно влияют накладные расходы, связанные с использованием потоков.

Далее рассмотрим учет рассмотренных выше факторов при разработке функции для умножения полиномов в алгоритме NTRU. Данная функция используется при генерации открытого ключа, шифровании и расшифровании. Операция умножения полиномов по сравнению с другими операциями, которые используются в алгоритме, имеет максимальную временную сложность.

Оптимизация алгоритма умножения полиномов для алгоритма NTRU. В алгоритме NTRU необходимо найти произведение полиномов, один из которых имеет коэффициенты 0, 1, -1 (вероятность каждого значения одинакова), а второй – коэффициенты в диапазоне [-1024, 1023]. Степени полиномов одинаковы. Результатом умножения полиномов является полином той же степени, его коэффициенты приводятся к интервалу [-1024, 1023].

Код для умножения полиномов (первый вариант)

```
void Mul0 (int *x, int *y, int *z, size_t n){
    size_t i, j;
    for (i = 0; i < n; ++i)    z [i] = 0;
    for (i = 0; i < n; ++i)
        for (j = 0; j < n; ++j)    {
            z [(i + j)%n] += x [i] * y [j];
            z [(i + j)%n]%=2048;
        }
}
```

Для оптимизации кода необходимо:

1 Оптимизировать последовательный вариант за счет

1.1 Минимизации длины данных с учетом их значений (более эффективное использование Кеша)

1.2 Уменьшения числа операций вычисления модуля (взятие по модулю возможно после выполнения умножения, а не на каждом шаге)

1.3 Переход от операции умножения на операции сложения – вычитания (с учетом значений коэффициентов первого полинома 1, -1, 0). Минимизация числа команд перехода, связанных с анализом этих значений.

1.4 Уменьшение числа команд перехода за счет уменьшения числа итераций, связанных с использованием блоков

2 Использовать параллельные вычисления

2.1 Использование команд SSE для вычисления промежуточных сумм и модулей

2.2 Использование Open MP для вычисления промежуточных сумм.

В табл. 6 приведены временные характеристики функции умножения полиномов в результате предложенных оптимизаций.

Заметим, что более эффективное использование кеша (1.1) за счет использования более коротких данных не существенно улучшило время

выполнения. Это связано с тем, что в обоих случаях полином и все промежуточные данные в кеше помещаются. Уменьшение числа операций вычисления модуля (1.2) существенно улучшило эффективность кода. Колонки табл. 6 1.3 и 1.4 показывают эффективность соответствующих преобразований. Суммарное ускорение за счет преобразований 1.1–1.4 составляет более 34 раз.

Таблица 6

Умножение усеченных полиномов ($n = 1499^4$)

	Mul0	1.1	1.2	1.3	1.4	2.1	2.2
Время (мс)	25.1	22.6	1.6	0.83	0.73	0.15	0.0466

Переход на параллельные вычисления (пункты 2.1 и 2.2) приводят также к увеличению эффективности кода. Суммарное ускорение от параллельных вычислений ускорило операцию умножения более, чем в 15 раз.

Общее ускорение, достигнутое для операции умножения полиномов, составляет более, чем 500 раз.

ЗАКЛЮЧЕНИЕ

Исследование, проведенное в данной работе, показывает, что для современных процессоров число операций не всегда является достаточным критерием для оценки эффективности алгоритмов. Так, при реализации пунктов 1.3, 1.4 было увеличено число операций для достижения минимизации переходов. Параллельные вычисления с помощью SIMD операций безусловно эффективны, но они применимы только для специфических задач. Эффективность параллельных вычислений с помощью потоков зависит от соотношения полезной работы и накладных расходов. В любом случае при разработке современных приложений необходимо обязательно учитывать рассмотренные особенности современных процессоров

Литература

- [1] <http://www.intel.com/content/dam/doc/manual/64-ia-32-architectures-optimization-manual.pdf>
- [2] A Chosen-Ciphertext Attack against NTRU. <http://www.iacr.org/archive/crypto2000/18800021/18800021.pdf>
- [3] OpenMP Application Program Interface. Version 4.0 - July 2013. <http://www.openmp.org/mp-documents/OpenMP4.0.0.pdf>
- [4] Efficiency Improvement for NTRU. Johannes Buchmann, Martin Döring, Richard Lindner. <https://www.cdc.informatik.tu-darmstadt.de/reports/reports/ntrusves.pdf>

Поступила в редколлегию 26.06.2014

⁴ Максимальная степень полинома в соответствии со стандартом 1499.



Качко Елена Григорьевна, кандидат технических наук, профессор кафедры ПО ЭВМ ХНУРЭ. Научные интересы: программные средства криптографических систем.



Балагура Дмитрий Сергеевич, кандидат технических наук, доцент кафедры безопасности информационных технологий ХНУРЭ. Научные интересы: защита информации, криптографические протоколы выработки и согласования ключей.



Погребняк Константин Анатольевич, доцент каф. БИТ ХНУРЭ, начальник отдела КЗИ АО «ИИТ». Научные интересы: применение методов алгебраической геометрии в криптологии, асимметричный криптоанализ.

УДК 004 056 55

Вплив властивостей сучасних процесорів на продуктивність програм / О. Г. Качко, Д. С. Балагура, К. А. Погребняк // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 281–285.

Здійснюється аналіз та порівняння способів оптимізації продуктивності програм. Наводяться теоретичні та експериментальні результати досліджень впливу на продуктивність конвеєрної обробки, кеш-пам'яті та розпаралелювання обчислень. Надається оцінка ефективності використання різних технологій для підвищення продуктивності та рекомендації щодо їх застосування.

Ключові слова: конвеєр, кеш-пам'ять, криптографічні перетворення, паралельні обчислення TBB, OpenMP.

Табл.: 6. Бібліогр.: 4 найм.

UDC 004 056 55

Influence of the properties of modern processors on program performance / O.G. Kachko, D.S. Balagura, K.A. Pogrebnyak // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 281–285.

An analysis and comparison of ways to optimize programs performance are carried out. Theoretical and experimental results of researches of the effect on the performance of pipelining, a cache memory, and parallel computing are provided. Assesses of the effectiveness of using different technologies to improve performance and recommendations for their use are given.

Keywords: pipeline, cache memory, cryptographic transformations, parallel computing, TBB, OpenMP.

Tab.: 6.: Ref.: 4 items.

КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ОЦЕНКА

УДК 681.3.06

ПОСТРОЕНИЕ КРИВОЙ ЭДВАРДСА НА БАЗЕ ИЗОМОРФНОЙ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В КАНОНИЧЕСКОЙ ФОРМЕ

А.В. БЕССАЛОВ

Получены условия существования канонических кривых, изоморфных кривым в форме Эдвардса над простым полем. Найдена зависимость параметра d кривой Эдвардса от параметров канонической кривой. Приведено новое доказательство для точных формул расчета числа кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами a и b .

Ключевые слова: каноническая эллиптическая кривая, кривая Эдвардса, кривая кручения, параметры кривой, изоморфизм, квадратичный вычет, квадратичный невычет.

ВВЕДЕНИЕ

Перспективным классом эллиптических кривых сегодня являются кривые в форме Эдвардса [1–6], рекордные по быстродействию и удобные для программирования. Двойная симметрия их в координатах поля характеристики $p > 2$ порождает четырехкратную избыточность по числу точек N_E . Так как $N_E \equiv 0 \pmod{4}$, циклические кривые Эдвардса всегда содержат одну точку 2-го порядка и две точки 4-го порядка. Кривых в канонической форме с таким свойством сравнительно немного, поэтому для построения изоморфных им кривых Эдвардса следует решить задачу поиска кривых в форме Вейерштрасса с двумя точками 4-го порядка. В работе [6] мы ввели зависимый от традиционных параметров (a, b) канонической кривой параметр c как единственный в поле F_p корень кубического уравнения. В ней получены системы линейных уравнений для неизвестных параметров a и c^2 с решениями, выраженными через квадратичные вычеты и невычеты. Для нахождения точного числа канонических кривых с ненулевыми параметрами, изоморфных форме Эдвардса, потребовалось сформулировать и доказать две леммы о числе решений уравнений, связывающих суммы вычетов и невычетов. Доказательства опираются на схему Гаусса распределения квадратичных вычетов. В итоге удалось найти формулы расчета точного числа кривых с заданными свойствами для любых $p \equiv 3 \pmod{4}$ и $p \equiv 1 \pmod{4}$.

В настоящей работе, опираясь на свойства кривых в канонической форме, автор нашел функциональную связь между параметром d кривой Эдвардса и параметрами изоморфной канонической кривой. Далее приводится новое более лаконичное доказательство утверждения, определяющего формулы расчета точного числа кривых Эдвардса, изоморфных кривым в форме Вейерштрасса с ненулевыми параметрами a и b . Кроме того, приведен алгоритм поиска изоморфных форме Эдвардса кривых, полезных для криптографии.

1. ОПРЕДЕЛЕНИЕ ФУНКЦИОНАЛЬНОЙ ЗАВИСИМОСТИ МЕЖДУ ПАРАМЕТРАМИ КРИВОЙ В ФОРМЕ ЭДВАРДСА И КАНОНИЧЕСКОЙ КРИВОЙ

Каноническая кривая над полем характеристики $p \neq 2, 3$ описывается известным уравнением [7]

$$E_p: y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0, a, b \in F_p. \quad (1)$$

Пусть c — единственный в поле F_p корень кубического уравнения $x^3 + ax + b = 0$, тогда вместо (1) можем записать

$$y^2 = (x - c)(x^2 + cx + a + c^2), \\ b = -c^3 - ac, c \in F_p. \quad (2)$$

Определим условия, накладываемые на параметры a и c , при которых имеется единственная точка 2-го порядка и 2 точки 4-го порядка. Второй задачей в этом разделе будет нахождение зависимости между параметрами a и c канонической формы эллиптической кривой и параметром d кривой $x^2 + y^2 = 1 + dx^2y^2$ в форме Эдвардса.

Примем $u = x - c$, тогда уравнение (3) представляется в форме Монтгомери [2,3]

$$y^2 = u(u^2 + 3cu + a + 3c^2). \quad (3)$$

Парабола в правой части (4) не имеет корней в поле F_p , если дискриминант квадратного уравнения является квадратичным невычетом, т.е.

$$9c^2 - 4(a + 3c^2) = -(3c^2 + 4a) \neq A^2. \quad (4)$$

Это условие гарантирует существование единственной точки 2-го порядка кривой (3), определяемой для (3) как $D = (0, 0)$. Условие $A^2 \neq 0$, входящее в (4), исключает появление кратных корней кубического уравнения и, тем самым, сингулярные кривые [7].

Пусть $P = (u_1, y_1)$ — точка 4-го порядка кривой (3). Ее удвоение $2P = D$ дает координаты точки $D = (0, 0)$. При удвоении мы строим касательную к кривой в точке P , которая проходит через точку $(0, 0)$. Таким образом из (3)

$$\frac{dy}{du}\bigg|_{u=u_1} = \frac{3u_1^2 + 6cu_1 + 3c^2 + a}{2u_1} = \frac{y_1}{u_1}$$

Отсюда

$$2y_1^2 = 3u_1^3 + 6cu_1^2 + (3c^2 + a)u_1. \quad (5)$$

С другой стороны, в этой же точке согласно (3) имеем

$$2y_1^2 = 2u_1^3 + 6cu_1^2 + 2(3c^2 + a)u_1. \quad (6)$$

Из системы уравнений (5), (6) получим квадраты для координат точки P 4-го порядка

$$u_1^2 = 3c^2 + a, \quad y_1^2 = 2u_1^3 + 3cu_1^2. \quad (7)$$

Из последнего выражения можно теперь получить

$$3c = \frac{y_1^2}{u_1^3} \left(1 - 2 \frac{u_1^3}{y_1^2} \right) u_1 = 2 \frac{1+d}{1-d} u_1 \quad (8)$$

где

$$d = 1 - 4 \frac{u_1^3}{y_1^2}. \quad (9)$$

Формулы (7), (9) позволяют выразить параметр d через параметры a и c канонической формы кривой

$$d = \frac{3c - 2u_1}{3c + 2u_1}, \quad u_1 = (-1)^\alpha \sqrt{3c^2 + a}, \quad \alpha \in \{0, 1\}. \quad (10)$$

Здесь с помощью двоичного α выбирается одно из решений квадратного уравнения u_1 , которое принадлежит кривой (3) и дает ровно две точки 4-го порядка. Второе решение не может лежать на кривой: это порождает четыре точки 4-го порядка, что нарушает структуру группы [7].

Из (4) и (7) следует, что необходимыми условиями существования одной точки 2-го и двух точек 4-го порядков являются следующие соотношения, выраженные через символы Лежандра как

$$a) \left(\frac{-(3c^2 + 4a)}{p} \right) = -1, \quad b) \left(\frac{(3c^2 + a)}{p} \right) = 1. \quad (11)$$

С учетом (7) и (8) и деления на u_1^3 уравнение (3) теперь может быть приведено к виду

$$\frac{1}{1-d} v^2 = u^3 + 2 \frac{1+d}{1-d} u^2 + u. \quad (12)$$

Эта форма кривой с помощью сравнительно несложной замены переменных $(u, v) \rightarrow (x, y)$ [2,3] приводится к кривой в форме Эдвардса

$$x^2 + y^2 = 1 + d x^2 y^2, \quad d \neq 0, 1, \quad \left(\frac{d}{p} \right) = -1. \quad (13)$$

Класс изоморфных кривых Эдвардса

$$X^2 + Y^2 = e^2 (1 + d^* X^2 Y^2), \quad d^* = e^{-4} d, \quad (14)$$

определяется линейной заменой переменных $x \rightarrow e^{-1} X, y \rightarrow e^{-1} Y$. Такая трансформация расширяет множество всех кривых в $(p-1)/2$ раз, но практически бесполезна (более того, добавление нового параметра e усложняет групповые операции).

Как нетрудно видеть из (12), заменой $d \rightarrow d^{-1}$ получаем кривую кручения с порядком

$N_E^t = p + 1 + t$, симметричным порядку $N_E = p + 1 - t$ исходной кривой относительно середины $p + 1$. Заметим, что для кривых Эдвардса порядок кривой $N_E = 0 \bmod 4$, поэтому след уравнения Фробениуса t может быть равен 0 лишь для значений модуля $p = 3 \bmod 4$. В этом случае элемент поля (-1) является квадратичным невычетом, и при значении $d = d^{-1} = -1$ пара кривых кручения вырождается в одну суперсингулярную кривую с порядком $N_E = p + 1$. Это следует также из уравнения (12), которое при $d = -1$ принимает вид $y^2 = u^3 + u$ [7]. В форме (1) это кривая с коэффициентом $b = 0$.

В криптографических приложениях не используются уязвимые к MOV-атаке кривые с нулевыми параметрами a или b . Возникает вопрос о числе кривых Эдвардса, изоморфных каноническим кривым с ненулевыми коэффициентами a и b . Эта задача получила точное решение в работе [6] на основе свойств параметров a и c канонических кривых, при этом нам пришлось сформулировать и доказать две леммы в теории квадратичных вычетов и теорему. В следующем разделе мы более лаконично докажем полученные в [6] результаты, опираясь в основном на свойства кривой в форме Эдвардса.

2. НОВОЕ ДОКАЗАТЕЛЬСТВО ДЛЯ РАСЧЕТА ТОЧНОГО ЧИСЛА КРИВЫХ ЭДВАРДСА, ИЗОМОРФНЫХ КРИВЫМ В КАНОНИЧЕСКОЙ ФОРМЕ С НЕНУЛЕВЫМИ ПАРАМЕТРАМИ A И B

Утверждение. Число кривых Эдвардса (14), изоморфных кривым (1) в канонической форме с параметрами $a \neq 0$ и $b \neq 0$ над полем F_p с двумя точками 4-го порядка определяется формулами:

I. При $p \equiv 3 \bmod 4$

$$(\alpha) M_\alpha = (p-1)(p-7)/4, \text{ если } \left(\frac{3}{p} \right) = 1;$$

$$(\beta) M_\beta = (p-1)(p-3)/4, \text{ если } \left(\frac{3}{p} \right) = -1;$$

II. При $p \equiv 1 \bmod 4$

$$(\gamma) M_\gamma = (p-1)^2/4.$$

Доказательство.

1. Пусть $p \equiv 3 \bmod 4$, тогда (-1) – квадратичный невычет [7], т.е. $\left(\frac{-1}{p} \right) = -1$ и для (11a) невычет заменяем квадратичным вычетом

$$\left(\frac{-1}{p} \right) \left(\frac{3c^2 + 4a}{p} \right) = \left(\frac{-1}{p} \right) \Rightarrow \left(\frac{3c^2 + 4a}{p} \right) = 1.$$

Аргументы символов Лежандра (11) являются линейными функциями параметров a и c^2 . Следовательно, имеем невырожденную систему двух линейных уравнений над полем F_p

$$3c^2 + 4a = A^2,$$

$$3c^2 + a = B^2,$$

с решениями:

$$a = 3^{-1}(A^2 - B^2), c^2 = 9^{-1}(4B^2 - A^2). \quad (15)$$

Для кривых с параметрами $a \neq 0$ и $b \neq 0$ квадратичные вычеты $A^2 \neq B^2$ и, кроме того, $4B^2 \neq A^2$ (нулевые вычеты c^2 отбрасываются, т. к. из $c = 0 \Rightarrow b = -c^3 - ac = 0$). Из (11) следует, что $A^2 \neq 0$ и $B^2 \neq 0$.

Так как параметр d в форме кривой Эдвардса (13) пробегает все квадратичные невычеты поля F_p , их число равно $(p-1)/2$. Из этого числа исключим значение $d = -1$, которое порождает коэффициенты $c = b = 0$ (см. формулы (1) и (10)). Остается $(p-3)/2$ квадратичных невычетов d .

Пусть $\left(\frac{3}{p}\right) = 1$. Из (15) следует, что при $a = 0$ $A^2 = B^2$ и $c^2 = 3^{-1}A^2$, т.е. существует решение для c и, соответственно, для параметра d , равного согласно (10)

$$d = \frac{3c \pm 2c\sqrt{3}}{3c \pm 2c\sqrt{3}} = \frac{\sqrt{3} \pm 2}{\sqrt{3} \pm 2}. \quad (16)$$

Нетрудно видеть, что оба решения (16) являются невычетами. Например, умножив числитель и знаменатель на знаменатель, получим в знаменателе квадрат, а в числителе разность квадратов $3 - 4 = -1$, т.е. невычет при $p \equiv 3 \pmod{4}$. Следовательно, из $(p-3)/2$ значений невычетов d , исключая значение $b = 0$, следует удалить еще 2 значения (16), порождающих коэффициент $a = 0$. При этом остается $(p-7)/2$ допустимых значений невычетов d . Для каждой кривой Эдвардса в форме (13) существует $(p-1)/2$ изоморфных кривых (14) с соответствующим числом квадратов e^2 . Общее число кривых Эдвардса с оговоренными свойствами равно $M_\alpha = (p-1)(p-7)/4$. Утверждение (α) доказано.

Пусть теперь $\left(\frac{3}{p}\right) = -1$. В этом случае $a \neq 0$, т. к. при $A^2 = B^2$ уравнение $c^2 = 3^{-1}A^2$ (см. (15)) не имеет решения. Тогда имеем $(p-3)/2$ допустимых значений невычетов d , которые вместе с $(p-1)/2$ значениями квадратов e^2 для изоморфных кривых дает $M_\beta = (p-1)(p-3)/4$ кривых. Утверждение (β) доказано.

2. Пусть теперь $p \equiv 1 \pmod{4}$, тогда $(-1) -$ квадратичный вычет, т.е. $\left(\frac{-1}{p}\right) = 1$. [7]. Тогда для (11a), принимая A невычетом в системе уравнений

$$3c^2 + 4a = A, \left(\frac{A}{p}\right) = -1. \\ 3c^2 + a = B^2,$$

можно найти ее единственное решение

$$\Rightarrow a = 3^{-1}(A - B^2), c^2 = 9^{-1}(4B^2 - A). \quad (17)$$

Здесь, как видим, нулевые решения для a и c^2 невозможны. Итак, мы имеем $(p-1)/2$ допустимых значений невычетов d , которые вместе с $(p-1)/2$ значениями квадратов e^2 для кривых в форме (14) дает $M_\gamma = (p-1)^2/4$ кривых. Утверждение (γ) доказано.

Можно заметить, что приведенное здесь доказательство формул, определяющих точное число кривых Эдвардса с оговоренными свойствами, существенно проще предыдущего доказательства [6].

Рассчитанные по формулам (α), (β), (γ) мощности семейств кривых, изоморфных кривым Эдвардса при значениях $p = 7, 11, 13, \dots, 47$ приведены в табл. 1.

Таблица 1

p	7	11	13	17	19	23	29	31	37	41	43	47
М	6	10	36	64	72	88	196	210	324	400	420	529

Пример. Требуется построить кривую Эдвардса на базе изоморфной канонической кривой с двумя точками 4-го порядка над полем F_7 . Примем $A^2 = 2$, $B^2 = 1$, тогда согласно (15) $c^2 = 1$ – квадрат в поле, $a = 5$ и $b = \pm c(c^2 + a) = \pm 1$. Получили пару кривых кручения $y^2 = x^3 + 5x \pm 1$ с порядками $N_E = 12$ и $N_E^t = 4$. Первая кривая с параметром $c = 1$ в форме Монтгомери (3) имеет вид $y^2 = u(u^2 + 3u + 1)$. Ее точка второго порядка $D = (0,0)$, а координаты точек 4-го порядка первой кривой в соответствии с (7) равны

$$u_1^2 = 3c^2 + a = 1 \Rightarrow u_1 = -1, \\ y_1^2 = 2u_1^3 + 3cu_1^2 = 1 \Rightarrow y_1 = \pm 1.$$

Здесь решение $u_1 = 1$, не лежащее на кривой (3), отбрасывается. Переход к кривой Эдвардса (13) осуществляется вычислением d согласно (10)

$$d = \frac{3+2}{3-2} = 5.$$

Кривая $x^2 + y^2 = (1 + 5x^2y^2) \pmod{7}$ имеет порядок 12. Соответствующая кривая кручения с параметром $d^{-1} = 3$ имеет порядок 4. Кривая с параметром $d = -1$ отбрасывается. Других кривых в форме (13) при $p = 7$ не существует. Для каждой из этих двух кривых можно получить по 3 изоморфных кривых (14) с коэффициентами $e^2 = 1, 4, 2$. Вообще над полем F_7 существует, как следует из таблицы 1, 6 кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами a и b и двумя точками 4-го порядка. Здесь каждая пара кривых кручения содержит по 3 изоморфных пар.

Формулы (15), (17) конструктивны, т. к. позволяют рассчитывать параметры a и $\pm c$ кривой (и, соответственно, $\pm b$) при заданных значениях пар квадратичных вычетов (A^2, B^2) .

На основе условий (11) и формул (15), (17) можно предложить следующий алгоритм построения канонических кривых с двумя точками 4-го порядка:

1. В поле F_p задаем произвольное значение пары квадратичных вычетов (A^2, B^2) или пары (A, B^2) и согласно (15) или (17) рассчитываем параметры a и c^2 . Если вычисленное значение c^2 – невычет, меняем параметр B^2 и повторяем расчеты.

2. Если c^2 – квадратичный вычет, находим 2 кривые с параметрами $(a, \pm c)$ и $(a, \pm b)$. Значение параметра b рассчитываем в соответствии с (2).

3. Находим координаты точки 4-го порядка (для построения изоморфной кривой Эдвардса).

4. Вычисляем порядок одной из кривых и, в случае неприемлемого порядка, рассчитываем порядок кривой кручения. Если решение не найдено, переходим к другой паре значений (A^2 , B^2) или (A , B^2) (возвращаемся в п.1).

В предложенном виде алгоритм достаточно быстро приводит к кривой с двумя точками 4-го порядка. Далее, как описано в данной работе, строится изоморфная кривая в форме Эдвардса.

Литература

- [1] *Edwards H.M.* A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393–422.
- [2] *Bernstein Daniel J., Lange Tanja.* Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007. — P. 1–20.
- [3] *Бессалов А.В.* Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. — С. 203–208.
- [4] *Бессалов А.В., Гурьянов А.И., Дихтенко А.А.* Кривые Эдвардса почти простого порядка над расширениями малых простых полей. Прикладная радиоэлектроника, том 11, № 2, 2012. — С. 225–227.
- [5] *Бессалов А.В., Дихтенко А.А.* Криптостойкие кривые Эдвардса над простыми полями. Прикладная радиоэлектроника, 2013, Том 12, №2. — С. 285–291.
- [6] *Бессалов А.В., Дихтенко А.А., Цыганкова О.В.* Плотность канонических эллиптических кривых со свойством изоморфизма к форме Эдвардса. Известия ЮФУ. Технические науки, вып. №4, 2014. — С. 146–153.
- [7] *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых: учеб. пособие. — К.: ИВЦ «Політехніка», 2004. — 224 с.

Поступила в редколлегию 6.06.2014



Бессалов Анатолий Владимирович, доктор технических наук, профессор, профессор кафедры ММЗИ ФТИ НТУУ «КПИ». Научные интересы: криптография, теория корректирующего кодирования.

УДК621.391.7:336.71

Побудова кривої Едвардса на базі ізоморфної еліптичної кривої у канонічній формі / А.В. Бессалов // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 286–289.

Отримано умови існування канонічних кривих, які ізоморфні кривим у формі Едвардса над простим полем. Знайдено залежність параметра d кривої Едвардса від параметрів канонічної кривої. Наведено новий доказ для точних формул розрахунку кількості кривих Едвардса, які є ізоморфними канонічним кривим з ненульовими параметрами a і b .

Ключові слова: канонічна еліптична крива, крива Едвардса, крива кручення, параметри кривої, ізоморфізм, квадратичний лишок, квадратичний нелишок.

Табл.: 01. Бібліогр.: 07 найм.

UDC 621.391.7:336.71

Construction of Edwards curve on the basis of an isomorphic elliptic curve in a canonical form / A.V. Bessalov // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 286–289.

Living conditions of canonical curves, isomorphic to curves in the Edwards form over a simple field, are established. The dependence of Edward curve parameters d on parameters of a canonical curve is found. A new proof for exact calculation formulae of Edwards curves number, isomorphic to canonical curves with nonzero parameters a and b is provided.

Keywords: canonical elliptic curve, Edwards curve, torsion curve, curve parameters, isomorphism, quadratic residue, non-quadratic residue.

Tab.: 01. Ref.: 07 items.

ПАРОЛЬ ЯК ФАКТОР БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

М.В. ЄСІНА, І.Д. ГОРБЕНКО, О.О. БАКЛИКОВ

Розглядаються методи та схеми багатофакторної автентифікації. Детально розглядається такий фактор багатофакторної автентифікації як «пароль». Аналізуються характеристики та формуються вимоги до обраного фактора.

Ключові слова: автентифікація, пароль, схема, фактор.

ВСТУП

Зараз у технологічно розвинених державах особливу увагу приділяють проблемам кібербезпеки, розроблено та реалізуються доктрини інформаційної безпеки. Основним змістом доктрин є протидія загрозам безпеки, насамперед — захисту від несанкціонованого доступу (НСД) до інформації та інформаційних ресурсів.

Забезпечення безпеки інформаційної системи є одним з найважливіших завдань в ході її експлуатації, оскільки від конфіденційності, цілісності та доступності інформаційних ресурсів багато в чому залежить швидкість прийняття рішень, ефективність і надійність роботи.

Незважаючи на безліч засобів обчислювальної техніки і широкий спектр технологічних рішень, вибір методів автентифікації для компаній, що планують своє майбутнє, не великий — швидше за все, необхідно використовувати механізми багатофакторної автентифікації. Багатофакторна автентифікація — це автентифікація з хоча б двома незалежними факторами автентифікації. При цьому можуть використовуватися фактори різної природи [4]:

- властивість, яку має суб'єкт (наприклад, біометричні дані);
- знання — інформація, яку має суб'єкт (наприклад, пароль чи пін-код);
- володіння — річ, яку має суб'єкт (наприклад, електронна або магнітна картка, флеш-пам'ять, електронний ключ).

Механізми автентифікації пов'язані із захистом інформації взагалі — повідомлень чи ресурсів, від їх модифікації, підміни чи створення хибних. Самі механізми автентифікації можна розглядати як заходи захисту, що призначені для встановлення достовірності передачі повідомлення чи відправника або засобів верифікації санкціонування індивідуума для отримання конкретних категорій інформації. По суті, автентифікація є процедурою чи процесом встановлення достовірності твердження, що суб'єкт або об'єкт має заявлені (очікувані) властивості. Механізми автентифікації можна розглядати як методи захисту в ІТС від різних видів обману її користувачів.

До переваг багатофакторної автентифікації можна віднести здатність захистити інформацію, як від внутрішніх загроз, так і від зовнішніх вторгнень.

Певною її слабкістю можна вважати необхідність використання додаткових програмно-апаратних комплексів, засобів зберігання і зчитування даних.

1. ПАРОЛЬНА АВТЕНТИФІКАЦІЯ

Дану автентифікацію реалізують за допомогою штатних програмних засобів операційних систем (ОС), систем управління базами даних (СУБД), моніторів телеобробки, мережних пакетів. Суть цієї автентифікації полягає в тому, що кожному зареєстрованому користувачеві видається персональний пароль, який він повинен тримати в таємниці та вводити в автоматизовану систему при кожному зверненні до неї. Спеціальна програма порівнює введений пароль із еталоном, що зберігається в пам'яті, і при збігу паролів запит користувача виконується [2].

Простота цього способу очевидна, але очевидні також і його явні недоліки: пароль можна підглянути, вкрати, дібрати перебиранням можливих комбінацій або проникнути в ту ділянку пам'яті, де зберігаються еталонні паролі (хоча сьогодні сучасні ОС, СУБД, як правило, зашифровують паролі різними способами) [2].

До заходів підвищення безпеки паролівних систем автентифікації, окрім згаданого зберігання списків паролів у зашифрованому вигляді, може бути віднесене скорочення термінів дії паролів аж до застосування паролів одноразового використання. Останнім часом для цілей автентифікації широко використовується так званий метод «запит—відповідь», який дозволяє не лише автентифікувати користувача, але й дає можливість користувачеві здійснювати автентифікацію системи, з якою він працює. Це має принципове значення під час роботи в мережі, оскільки використання підставного комп'ютера, ОС або програми є одним зі шляхів несанкціонованого отримання повідомлень або паролів законних користувачів. Слід зазначити, що необхідність такої взаємної автентифікації підтверджена міжнародним стандартом із взаємодії відкритих систем. Різновидом такої автентифікації є і так зване впізнання в діалоговому режимі, здійснюване за наступною схемою. У файлах механізмів захисту завчасно створюються записи, що персоналізують дані користувача (дата народження, імена й дати народження і т.д.) або чималий і впорядкований набір паролів. При зверненні користувача

програма захисту пропонує йому назвати деякі дані з наявного запису, які порівнюються з тими, що зберігаються у файлі. За результатами порівняння приймається рішення про допуск. Для підвищення надійності впізнання запитувані в користувача дані можуть вибиратися щоразу різні [2].

Практичне застосування механізму паролювання можна розглянути на прикладі БД MS Access. При підключенні до БД потребується ввести пароль (рис. 1). Після вводу пароля можливі два випадки: якщо введений пароль є правильним (рис. 2), то відбувається підключення до БД, якщо ні, то програма видає повідомлення про помилковий пароль і подальша робота з БД стає неможливою (рис. 3).

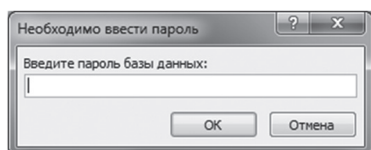


Рис. 1. Вікно введення пароля при підключенні до БД

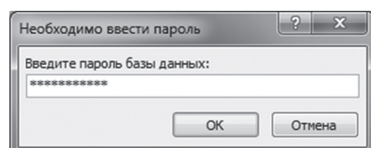


Рис. 2. Введення пароля (пароль правильний)

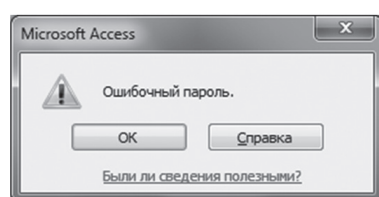


Рис. 3. Введення пароля (помилковий пароль)

2. МЕТОДИ ЗЛОМУ ПАРОЛІВ

1. Атака з використанням словників.

При зломі паролів з використанням словників використовується простий файл, що містить слова, які можна знайти в словнику. Іншими словами, атаки такого типу перебирають саме слова, які багато людей використовують як пароль.

Така “хитрість”, як уміло згруповані разом слова, наприклад, “сісімвідкрийся” або “ясуперадміністратор”, не врятують пароль від злому — можливо, хакери всього лише витратять кілька зайвих секунд [6].

2. Атака методом повного перебору (грубої сили).

Цей метод схожий на атаку зі словником, але з доповненням — він дозволяє виявити слова, що не містяться в словнику, перебираючи всі можливі буквено-цифрові комбінації від aaa1 до zzz10.

Це не швидкий спосіб, особливо, якщо пароль складається з декількох символів, але, в кінцевому рахунку, пароль буде розкритий. Метод повного перебору може бути спрощений за допомогою використання додаткових обчислюваль-

них потужностей комп'ютера, в тому числі, з використанням можливостей відеокарти GPU — і, наприклад, використання розподілених обчислювальних моделей і зомбі-ботнетів [6].

3. Атака з використанням райдужної таблиці.

Райдужна таблиця — це список попередньо обчислених геш-значень (числових значень зашифрованих паролів), використовуваних більшістю сучасних систем. Таблиця включає в себе геш-значення всіх можливих комбінацій паролів для будь-якого виду алгоритму гешування. Час, необхідний для злому пароля за допомогою райдужної таблиці, зводиться до того часу, який потрібен, щоб знайти захешований пароль у списку. Тим не менше, сама таблиця має значний обсяг і для перегляду вимагає серйозних обчислювальних потужностей. Також ця таблиця не принесе очікуваних результатів, якщо геш-значення, яке вона намагається знайти, було ускладнено додаванням випадкових символів до пароля перед застосуванням алгоритму гешування [6].

4. Фішинг.

Найпростіший спосіб злому — запитати у користувача його пароль. Фішингове повідомлення переводить користувача на підроблені сайти онлайн-банкінгу, платіжних систем або інші сайти, на яких потрібно обов'язково ввести особисті дані [6].

5. Соціальна інженерія.

Соціальна інженерія дотримується тієї ж концепції, що і фішинг — “запитати у користувача пароль”, але не за допомогою поштової скриньки, а в реальному світі.

Одним зі способів соціальної інженерії є за-телефонувати в офіс під виглядом співробітника ІТ-безпеки і запитати пароль доступу до мережі [6].

6. Шкідливе програмне забезпечення.

Програма перехоплення інформації, що вводиться з клавіатури або виводиться на екран, може бути встановлена шкідливим ПЗ, яке фіксує всю інформацію, яку вводять користувач, або створює скріншоти під час процесу авторизації, а потім направляє копію цього файла зловмисникам.

Деякі шкідливі програми здійснюють пошук існуючого файла з пароллями веб-браузера клієнта, потім копіюють цей файл, який (крім зашифрованих) міститиме легкодоступні збережені паролі з історії сторінок, відвіданих користувачем [6].

7. Оффлайн хакінг.

Паролі знаходяться у безпеці, якщо вони захищені системою блокування (блокують дії користувачів після трьох-чотирьох невдалих спроб набору пароля). Зазначене також дозволяє блокувати програми автоматичного підбору паролів. Це було б правильно, якби не той факт, що більшість зломів паролів відбувається в оффлайн, з використанням набору хешей у файлі паролів, які були “отримані” від скомпрометованої системи.

Часто, розглянутий користувач виявляється скомпрометованим через злом третьої сторони, яка тим самим забезпечує доступ зловмисникам до системи серверів і всіх важливих файлів користувача з хешованими паролями. Зломщик паролів може працювати стільки часу, скільки йому потрібно, щоб спробувати зламати код без оповіщення цільової системи або окремих користувачів [6].

8. «Підглядання через плече». Найбільш скомпрометовані хакери під виглядом кур'єрів, фахівців з технічного обслуговування кондиціонерів або будь-яких інших службовців проникають в офісні будівлі. Як тільки вони потрапляють до офісної будівлі, уніформа обслуговуючого персоналу надає їм свого роду безкоштовний квиток на безперешкодний доступ у всі куточки офісної будівлі. Це дозволяє їм записувати паролі, що вводяться реальними співробітниками, а також надає відмінну можливість побачити всі ті паролі, що використовують легальні користувачі [6].

9. Метод “павуків”.

Відомо, що багато корпоративних паролів складаються зі слів, які пов'язані з бізнесом. Вивчення корпоративної літератури, матеріалів веб-сайтів, сайтів конкурентів і навіть список клієнтів можуть забезпечити хакерів інформацією для побудови користувацького списку слів, який потім використовується для злому методом грубої сили.

Дійсно, досвідчені хакери можуть формувати так звані “павутинні” додатки, аналогічні тим, які застосовуються провідними пошуковими системами, щоб визначити ключові слова, зібрати і обробити списки для злому [6].

10. Згадки.

Фактором, що використовується зломщиками паролів, звичайно, є передбачуваність у діях користувачів. Якщо дійсно випадковий пароль був створений за допомогою ПЗ, призначеного для цієї задачі, то користувацький «випадковий» пароль, навряд чи володітиме властивостями випадковості. Замість цього, завдяки емоційній прихильності користувачів до речей, які подобаються, швидше за все, ті «випадкові» паролі, які утворюються, будуть засновані на інтересах, хобі, іменах домашніх тварин, сім'ї тощо. Зломщики паролів, цілком імовірно, дізнавшись цю інформацію, зроблять кілька, часто правильних, здогадок при спробі зламати пароль споживчого рівня, не вдаючись до словника або методу грубої сили [6].

3. ПРОГРАМИ ДЛЯ ЗЛОМУ ПАРОЛІВ ТА ЇХ КЛАСИФІКАЦІЯ

Принцип роботи усіх програм, що дозволяють зламувати паролі, практично однаковий — відмінності лише у деталях. Існує два базових алгоритми злому паролів. Перший полягає в тому, щоб підбирати не сам пароль до документа, а саме секретний ключ і відповідно розшифровувати документ без знання його пароля. Такий тип атаки по ключу називається *keyspace attack* [7].

Другий алгоритм — це підбір пароля. Різні утиліти забезпечують різну швидкість перебору пробних паролів, у них можуть бути реалізовані і різні алгоритми генерації пробних паролів (типи атак). Традиційно виділяють три типи атак на паролі [7]:

- атака за словником;
- атака методом послідовного перебору;
- атака по масці.

Утиліти підбору паролів можна умовно розбити на два класи: багатоцільові програмні пакети, що дозволяють підбирати паролі до різного типу файлів, і спеціалізовані утиліти, які орієнтовані на підбір паролів до файлів, які створені якимось одним додатком. Фактично багатоцільові програмні пакети становлять собою збірник окремих утиліт (іноді такі пакети передбачають використання єдиної програмної оболонки для доступу до окремих утиліт) [7].

На сьогодні найбільш поширеними програмами для злому паролів є програми для злому: соціальних мереж, електронної пошти, різноманітних мережних ігор, платіжних систем, сайтів, Wi-Fi, користувацьких паролів, архівів, СУБД, Skype, ICQ і т.д.

Такі програми поділяються на безкоштовні, умовно безкоштовні та платні. З безкоштовними потрібно бути досить обережними — є досить високий ризик того, що вони можуть бути носіями шкідливого ПЗ.

4. СХЕМИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ФАКТОРА «ПАРОЛЬ» ТА ОЦІНКА ЙМОВІРНОСТІ НСД У ТАКИХ СХЕМАХ

Важливим питанням є оцінка безпеки схем багатофакторної автентифікації. В процесі побудови системи захисту від НСД спочатку необхідно визначити перелік факторів, які можна використовувати для здійснення багатофакторної автентифікації. Для захисту від НСД інформації та ресурсів з використанням певних факторів автентифікації необхідно визначити повний перелік атак зі сторони існуючих чи потенційних криптоаналітиків (порушників), зробити їх класифікацію, вибрати критерії та показники, які дозволили б порівняти їх та вибрати такі атаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД [1].

Найсильнішою схемою автентифікації є багатофакторна автентифікація, яка поєднує в собі використання криптографічних та біометричних методів.

Як основні показники захисту від НСД можна визначити такі [1]:

- 1) $P_{НСД}(n)$ — ймовірність НСД у n спробах, де n — кількість спроб отримати НСД;
- 2) t_6 — безпечний час;

3) $\Delta T = T_D$ — допустимий час НСД;

4) n — кількість спроб, які можливо здійснити.

Аналіз використання схем багатфакторної автентифікації показує, що в ході їх побудови можуть використовуватися механізми з послідовним, паралельним або комбінованим з'єднанням елементів, які реалізують фактори автентифікації. Також кількість елементів у схемі може змінюватися, вона залежатиме від призначення системи, що захищається та вимог до неї [4].

У випадку використання в багатфакторному механізмі автентифікації двох факторів, можливі такі комбінації: пароль(і) та ключ(і), пароль(і) і біометрична ознака(и), ключ(і) і біометрична ознака(и) [5].

В табл. 1 наведено часткові випадки моделей оцінки для трьох варіантів двофакторного механізму. В першому рядку наведено значення, які відповідають моделі, наведеній на рис. 4.

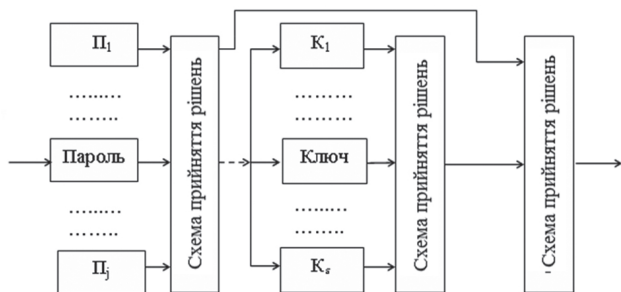


Рис. 4. Комбінована схема багатфакторної автентифікації «пароль і ключ»

Таблиця 1

Співвідношення для оцінки $P_{НСД}(P_{зах})$ механізмів комбінованої двофакторної автентифікації

Механізм пароль/ключ	$P_{НСД} = \left(1 - \prod_{i=1}^j P_i^n\right) \left(1 - \prod_{d=1}^{\epsilon} P_d^k\right)$
Механізм пароль/біометрія	$P_{НСД} = \left(1 - \prod_{i=1}^j P_i^n\right) \left(1 - \prod_{l=1}^{\mu} P_l^b\right)$
Механізм ключ/біометрія	$P_{НСД} = \left(1 - \prod_{d=1}^{\epsilon} P_d^k\right) \left(1 - \prod_{l=1}^{\mu} P_l^b\right)$
Механізм пароль/ключ	$P_{зах} = \prod_{i=1}^j P_i^n \cdot \prod_{j=1}^{\epsilon} P_j^k$
Механізм пароль/біометрія	$P_{зах} = \prod_{i=1}^j P_i^n \cdot \prod_{l=1}^{\mu} P_l^b$
Механізм ключ/біометрія	$P_{зах} = \prod_{j=1}^{\epsilon} P_j^k \cdot \prod_{l=1}^{\mu} P_l^b$

P^n — імовірність правильної роботи механізму паролювання, P^k — імовірність правильного застосування механізму ключа, P^b — імовірність правильного застосування механізму біометричних даних.

Також практичне значення мають окремі випадки, коли застосовується один або два фактори автентифікації у послідовному з'єднанні [5]. У табл. 2 наведено окремі випадки моделей оцінки для трьох варіантів двофакторного меха-

нізму автентифікації. На рис. 5 зображена схема послідовного з'єднання двофакторного механізму автентифікації «пароль і ключ» [3].



Рис. 5. Схема послідовного з'єднання двофакторного механізму захисту від НСД «пароль і ключ»

Таблиця 2

Співвідношення для оцінки $P_{НСД}(P_{зах})$ механізмів послідовної двофакторної автентифікації

Механізм пароль/ключ	$P_{НСД} = (1 - P_n)(1 - P_k)$
Механізм пароль/біометрія	$P_{НСД} = (1 - P_n)(1 - P_b)$
Механізм ключ/біометрія	$P_{НСД} = (1 - P_k)(1 - P_b)$
Механізм пароль/ключ	$P_{зах} = 1 - (1 - P_n)(1 - P_k)$
Механізм пароль/біометрія	$P_{зах} = 1 - (1 - P_n)(1 - P_b)$
Механізм ключ/біометрія	$P_{зах} = 1 - (1 - P_k)(1 - P_b)$

Як паролі можуть використовуватися паролі з m значною абеткою та довжиною пароля l_n , при чому пароль краще передавати у вигляді його геш-значення. У цьому випадку підвищується захищеність системи паролювання від компрометації фактичного значення пароля [3].

Ймовірність НСД $P_{НСД}$ до пароліної системи визначається таким чином [1]:

$$P_{НСД} \approx \frac{n}{m^{l_n}},$$

де m — основа алфавіту, l_n — довжина пароля, n — кількість спроб отримати НСД.

Таблиця 3

Значення $P_{НСД}$ для системи «пароль+ключ»

$P_{НСД}^n \backslash P_{НСД}^k$	10^{-19}	10^{-32}
$3,9 \times 10^{-3}$	$3,9 \times 10^{-22}$	$3,9 \times 10^{-35}$
$3,73 \times 10^{-9}$	$3,73 \times 10^{-28}$	$3,73 \times 10^{-41}$
$1,778 \times 10^{-13}$	$1,778 \times 10^{-32}$	$1,778 \times 10^{-45}$
$5,42 \times 10^{-20}$	$5,42 \times 10^{-39}$	$5,42 \times 10^{-52}$
$2,94 \times 10^{-39}$	$2,94 \times 10^{-58}$	$2,94 \times 10^{-71}$
$1,59 \times 10^{-58}$	$1,59 \times 10^{-77}$	$1,59 \times 10^{-90}$

Для забезпечення надійної роботи механізму паролювання значення $P_{НСД}$ мають задовольняти нерівності $P_{НСД} \leq 10^{-(6,-12,-16)}$. Також встановлено такі параметри та обмеження [3]:

1) при $n=1$ прийнятні значення $P_{НСД}$ характерні для $l \geq 8$, а $m=10,16,32,64$;

2) при $n=16$ прийнятні значення $P_{НСД}$ характерні для $l \geq 12$, $m=10,16,32,64$ та для значення $l=8$, коли $m > 16$;

3) при $n=2^{32}$ прийнятні значення $P_{НСД}$ характерні для $l \geq 16$, а $m=10,16,32,64$ та для значення $l=12$, коли $m \geq 32$;

4) при $n = 2^{64}$ прийнятні значення $P_{\text{НСД}}$ характерні для $l \geq 32$, а $m = 10, 16, 32, 64$ та для значення $l = 16$, коли $m \geq 64$;

5) при $n = 3 \times 10^{12}$ прийнятні значення $P_{\text{НСД}}$ характерні для $l \geq 32$, а $m = 10, 16, 32, 64$ та для значення $l = 16$, коли $m \geq 32$, а також для значення $l = 12$, коли $m \geq 64$.

5. ПРОГРАМНА МОДЕЛЬ ГЕНЕРАЦІЇ ПАРОЛІВ

Програмну модель для генерування паролів було реалізовано за допомогою пакета прикладного програмування MathCad15.

Було згенеровано чотири послідовності: за допомогою вбудованого генератора випадкових чисел, на основі m -послідовності та на основі послідовностей, сформованих за допомогою LLR і LCG. Для всіх отриманих послідовностей були проведені тести на випадковість і всі послідовності пройшли тест.

Для отримання з числових послідовностей символічних паролів, було реалізовано такі функції:

Функция формирования последовательности (для формирования пароля) всей длины на основе исходной последовательности (случай двоичной последовательности):

```
PWD(x) :=
  for i ∈ 0..  $\frac{\text{rows}(x)}{8} - 1$ 
  |  $v_i \leftarrow B\_D(\text{submatrix}(x, i \cdot 8, i \cdot 8 + 7, 0, 0))$ 
  |  $w_i \leftarrow v_i$  if  $(33 < v_i < 126)$ 
  |  $w_i \leftarrow \text{floor}(\text{runif}(1, 33, 126))_0$  otherwise
  | w
```

Функция формирования последовательности (для формирования пароля) всей длины на основе исходной последовательности (случай десятичной последовательности):

```
PWD_1(x) :=
  num ← floor(runif(1, 0, длина(x) - 8))_0
  for i ∈ 0.. 7
  |  $v \leftarrow \text{submatrix}(x, \text{num}, \text{num} + 7, 0, 0)$ 
  |  $w_i \leftarrow v_i$  if  $(33 < v_i < 126)$ 
  |  $w_i \leftarrow \text{floor}(\text{runif}(1, 33, 126))_0$  otherwise
  | w
```

Функция формирования последовательности для создания пароля, равной длине пароля:

```
pass(x) :=
  num ← floor(runif(1, 0, длина(x) - 8))_0
  p ← submatrix(x, num, num + 7, 0, 0)
  | pass ← p
```

Ці функції були застосовані до вихідних послідовностей і отримано паролі, які потім було записано до файла:

```
pwd_1 := password(plainText)
```

```
pwd_1T = (65 106 39 87 51 103 92 89)
```

```
vec2str(pwd_1) = "AjW3g\Y"
```

```
WRITEBIN("e:\УНИВЕР\АСПИРАНТУРА\Статьи\Статья в Радио
```

```
Электроника (пароли)\password_pwd_1.txt", "byte", 1) := pwd_1
```

Отриманий файл з паролем можна передавати користувачу для експлуатації. При передачі цей файл можна також захистити від зловмисників. Захист можна реалізувати за допомогою шифрування файла за допомогою будь-якого криптоалгоритму чи використовуючи стеганографічні методи.

ВИСНОВКИ

Як основні фактори автентифікації можна використовувати: властивість, яку має суб'єкт; знання — те, що знає суб'єкт; володіння — сутність, яку має суб'єкт.

Для кожного із факторів автентифікації необхідно визначити повний перелік атак зі сторони атакуючих чи потенційних криптоаналітиків (порушників), сформулювати критерії та показники, які дозволили б їх порівняти та обрати такі атаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД, тобто максимального значення $P_{\text{НСД}}$, потім сформулювати пропозиції та рекомендації, в тому числі для застосування у механізмах багатофакторної автентифікації.

Для забезпечення надійної роботи механізму паролювання значення $P_{\text{НСД}}$ мають задовольняти нерівності $P_{\text{НСД}} \leq 10^{-(6, -12, -16)}$. Також встановлено такі параметри та обмеження:

1) при $n = 1$ прийнятні значення $P_{\text{НСД}}$ характерні для $l \geq 8$, а $m = 10, 16, 32, 64$;

2) при $n = 16$ прийнятні значення $P_{\text{НСД}}$ характерні для $l \geq 12$, $m = 10, 16, 32, 64$ та для значення $l = 8$, коли $m > 16$;

3) при $n = 2^{32}$ прийнятні значення $P_{\text{НСД}}$ характерні для $l \geq 16$, а $m = 10, 16, 32, 64$ та для значення $l = 12$, коли $m \geq 32$;

4) при $n = 2^{64}$ прийнятні значення $P_{\text{НСД}}$ характерні для $l \geq 32$, а $m = 10, 16, 32, 64$ та для значення $l = 16$, коли $m \geq 64$;

5) при $n = 3 \times 10^{12}$ прийнятні значення $P_{\text{НСД}}$ характерні для $l \geq 32$, а $m = 10, 16, 32, 64$ та для значення $l = 16$, коли $m \geq 32$, а також для значення $l = 12$, коли $m \geq 64$.

Література

- [1] Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: монографія. — Харків: «Форт», 2012. — 870 с.
- [2] Єсін В.І., Кузнецов О.О., Сорока Л.С. Безпека інформаційних систем і технологій. — Харків: ХНУ імені В.Н. Каразіна, 2013. — 632 с.
- [3] Єсіна М.В., Горбенко І.Д. Багатофакторна автентифікація: використання механізмів двофакторної автентифікації для захисту від несанкціонованого доступу // Компьютерное моделирование в наукоемких технологиях (КМНТ-2014): Труды научнотехнической конференции с международным участием, 28-31 мая 2014 г. — Харьков: Харьковский национальный университет им. В.Н. Каразина, 2014. — С. 159–162.
- [4] Симонс Г.Д. Обзор методов аутентификации информации. — Москва: ТИИЭР, 1988. — Т. 76, №5. — С. 105–125.
- [5] Столлинес В. Криптография и защита сетей. Принципы и практика. 2-е изд. Москва: Вильямс, 2001. — 672 с.
- [6] [Електронний ресурс] — Режим доступу: <http://www.pcidss.ru/articles/39.html>
- [7] [Електронний ресурс] — Режим доступу: <http://compress.ru/article.aspx?id=18760>

Надійшла до редколегії 9.06.2014



Єсіна Марина Віталіївна, молодший науковий співробітник факультету комп'ютерних наук, кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: криптографія, криптоаналіз та їх застосування з метою захисту інформації, методи багатофакторної автентифікації та їх застосування з метою захисту інформації.

Горбенко Іван Дмитрович, фото та відомості про автора див. на стор. 216.



Бакликов Олександр Олександрович, інженер з систем захисту інформації в АТ «Інститут інформаційних технологій». Наукові інтереси: проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

УДК 004.056.55

Пароль как фактор многофакторной аутентификации / М.В. Есина, И.Д. Горбенко, А.А. Бакликов // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 290–295.

Рассматриваются методы и схемы многофакторной аутентификации. Детально рассматривается такой фактор многофакторной аутентификации как «пароль». Анализируются характеристики и формулируются требования к выбранному фактору.

Ключевые слова: аутентификация, пароль, схема, фактор.

Ил. 5. Библиогр.: 7 назв.

UDC 004.056.55

Password as a factor of multifactor authentication / M.V. Yesina, I.D. Gorbenko, O.O. Baklikov // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 290–295.

Multifactor authentication methods and schemes are considered. A “password” as a factor of multifactor authentication is considered in detail. Characteristics are analyzed and requirements to the selected factor are formulated.

Keywords: authentication, password, scheme, factor.

Fig. 5. Ref.: 7 items.

МЕТОД ПРОТИДІЇ ПЕРЕБОРУ ПАРОЛІВ, ЩО НЕ СТВОРЮЄ ВРАЗЛИВОСТІ ПОРУШЕННЯ ДОСТУПНОСТІ

А.О. БОЙКО

Запропоновано метод протидії перебору паролів. Запропонований метод не створює вразливості для атак порушення доступності системи, що оснований на блокуванні системи після кількох невдалих спроб автентифікації.

Ключові слова: пароль, перебір паролів, підбір паролів, доступність, плече атаки.

ВСТУП

Метод автентифікації по паролях використовується у багатьох програмних та апаратних засобах. У зв'язку з тим, що ентропія паролів є низькою, актуальним питанням є захист від атак перебору паролів.

Найбільш поширеним методом протидії перебору є блокування можливості введення паролів на певний час після заданої кількості неправильно введених паролів. Однак такий метод створює іншу вразливість — можливість порушення доступності інформації, яка захищається паролем, з боку неавтентифікованого користувача. У деяких системах та засобах ситуація погіршується тим, що блокування після перевищення порогу кількості неправильно введених паролів є безстроковим — або потребується втручання адміністратора, або інформація знищується.

Прикладом є смарт-картки, у яких після трьох разів неправильно введеного PIN відбувається знищення ключів. Водночас використовувати смарт-картки без такого механізму захисту використовувати небезпечно через те, що PIN має довжину 4–7 цифр (кількість варіантів $10^4 - 10^7$), що може бути легко підібрано.

1. АКТУАЛЬНІСТЬ

При рекомендованих компанією Microsoft налаштуваннях операційної системи Windows XP SP2 [1] визначено, що можливість автентифікації має блокуватися на 30 хв. після п'яти спроб введення неправильних паролів підряд. Якщо припустити, що на введення пустого пароля потрібно не більше 5 с, то лише за $5 \cdot 5 = 25$ с порушник може заблокувати робочу станцію на 30 хв., що у окремих випадках може бути небезпечно. Прикладом можуть бути автоматизовані системи керування технологічними процесами.

Під час проведення державної експертизи у сфері технічного захисту інформації операційної системи Windows XP SP2 цю небезпеку було відзначено [2] і рекомендовано блокувати можливість автентифікації після 50 спроб введення неправильних паролів підряд. Таким чином, на блокування доступу до робочої станції порушник повинен буде витратити 250 с, що все одно є практично можливим.

2. МЕТОД ПРОТИДІЇ АТАКАМ НА ДОСТУПНІСТЬ

У даній роботі запропоновано метод протидії перебору паролів, що не створює вразливості порушення доступності.

Основним показником атак, спрямованих на порушення доступності, є плече атаки. Плечем атаки називається відношення кількості ресурсів, які стають недоступними внаслідок атаки, до кількості ресурсів, які порушник повинен витратити на атаку. Чим менший цей показник, тим більш стійкою до атаки є система або засіб. У даному випадку ресурсом є час, і плече атаки при рекомендованих компанією Microsoft налаштуваннях операційної системи Windows XP SP2 складає $N = \frac{30 \cdot 60}{5 \cdot 5} = 72$.

Для смарт-карток плече атаки взагалі є нескінченним, оскільки при перевищенні кількості неправильно введених підряд PIN вони переходять у стан, з якого не можуть бути повернуті.

Для протидії таким атакам запропоновано динамічно збільшувати час між спробами введення пароля, а саме подвоювати час очікування наступної спроби після кожного неправильно введеного пароля. Щодо часу, який порушник повинен витратити на введення пароля, то можна зробити припущення на користь порушника і знехтувати цим часом.

Нехай після першої спроби система дозволить наступну спробу автентифікації після проміжку часу t . Тоді після другої спроби система дозволить наступну спробу автентифікації після проміжку часу $2t$. Після n спроб система дозволить наступну спробу автентифікації після проміжку часу $2^{n-1}t$. Саме цей час є часом, на який порушник може заблокувати систему, тобто $t_{dos} = 2^{n-1}t$. Водночас сам порушник повинен витратити час

Нехай після першої спроби система дозволить наступну спробу автентифікації після проміжку часу t . Тоді після другої спроби система дозволить наступну спробу автентифікації після проміжку часу $2t$. Після n спроб система дозволить наступну спробу автентифікації після проміжку часу $2^{n-1}t$. Саме цей час є часом, на який порушник може заблокувати систему, тобто $t_{dos} = 2^{n-1}t$. Водночас сам порушник повинен витратити час

$$t_{spent} = \begin{cases} 0, & n = 1 \\ \sum_{i=0}^{n-2} 2^i t, & n > 1 \end{cases}$$

Плече атаки складає

$$N = \frac{t_{dos}}{t_{spent}} = \frac{2^{n-1}t}{\sum_{i=0}^{n-2} 2^i t} = \frac{2^{n-1}}{\sum_{i=0}^{n-2} 2^i} = \frac{2^{n-1}}{2^{n-1} - 1}.$$

Зі зростанням кількості спроб плече атаки наближається до одиниці.

$$\lim_{n \rightarrow \infty} N = 1.$$

Фактично, порушник для порушення доступності системи або засобу на заданий час повинен витратити такий же час на атаку, що є не ефективним з точки зору порушника.

Реалізація даного методу не є складною і потребує лише двох змінних у програмі (регістрів у апаратурі) до 32 біт кожен і тактового генератора (годинника) з періодом $t = 1c$. Реалізація регістрів у енергонезалежній пам'яті дозволить створити смарт-картки, які не потрібно буде блокувати при спробах перебору PIN, оскільки вимкнення і повторне увімкнення живлення не скидає лічильники, отже не дозволить порушнику перебирати PIN занадто швидко. Водночас метод не створює незручностей звичайним користувачам, які вводять неправильний пароль або PIN 1–2 рази помилково.

ВИСНОВКИ

Запронований метод дозволяє ефективно протистояти перебору паролів, оскільки час, який витрачає порушник, експоненційно зростає.

Запронований метод не створює вразливості порушення доступності системи або засобу через блокування, викликане перевищенням кількості неправильно введених паролів.

Запронований метод не створює незручностей звичайним користувачам, які вводять неправильний пароль помилково.

Запронований метод є простим для програмної та апаратної реалізації.

Література

1. Windows XP Professional SP2 Security Guide – Режим доступу: <http://www.microsoft.com/en-us/download/confirmation.aspx?id=962>

2. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2. Інсталяція об'єкта експертизи та конфігурування параметрів безпеки – Режим доступу: http://msdb.com.ua/Downloads/Ukraine/Security/Expert/Conf_WXP_ver27_10_06.doc

Надійшла до редколегії 19.06.2014



Бойко Артем Олександрович, кандидат технічних наук. Наукові інтереси: принципи побудовання геш-функцій та використання їх у засобах захисту інформації.

УДК 621.391:519.2:519.7

Метод противодействия перебору паролей, который не создает уязвимостей нарушения доступности / А.А. Бойко // Прикладная радиоэлектроника: науч.-техн. журнал. — 2014. — Том 13. — № 3. — С. 296–297.

Предложен метод противодействия перебору паролей. Предложенный метод не создает уязвимости к атакам нарушения доступности системы, основаным на блокировании системы после нескольких неудачных попыток аутентификации.

Ключевые слова: пароль, перебор паролей, подбор паролей, доступность, плечо атаки.

Библиогр.: 2 назв.

UDC 621.391:519.2:519.7

Method of preventing password bruteforcing which does not create vulnerability to accessibility violation / A.O. Boiko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 296–297.

The method of preventing password bruteforcing is proposed. The proposed method does not create vulnerability to attacks of violating system accessibility which are based on blocking the system after a few failed authentication attempts.

Keywords: password, bruteforcing, selection of paroles, accessibility, attack ratio.

Ref.: 2 items.

ЗАГАЛЬНА АТАКА НА NTRUENCRYPT НА ОСНОВІ ПОМИЛОК РОЗШИФРУВАННЯ

К.А. ПОГРЕБНЯК, Д.С. ДЕНИСОВ

NTRUEncrypt — це криптографічна система з відкритим ключем, яка була створена як альтернатива RSA та криптосистем на еліптичних кривих (ECC). Виключними особливостями NTRU є оригінальний і специфічний математичний апарат та висока швидкість перетворень. Застосування NTRU можливо за умови, що на неї не існує криптоаналітичних атак, які здатні суттєво понизити її криптографічну стійкість. Метою цієї статті є аналіз захищеності криптосистеми від загальної атаки на основі помилок розшифрування.

Ключові слова: NTRU, помилки при розшифруванні, загальна атака на основі помилок розшифрування.

1. СУТНІСТЬ ОСНОВНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Усі операції відбуваються у кільці $R = \mathbb{Z}[X]/(X^N - 1)$, яке має назву кільця зрізаних поліномів. N вважається розміром кільця R . Детально опис криптоперетворень наведено у [1, 3].

Позначимо *шириною* (*Width*) *полінома* різницю між його найбільшим та найменшим коефіцієнтами.

Для генерації ключової пари використовуються поліноми f та g . Особливістю цих поліномів є те, що вони мають маленьку *ширину*. Зазвичай це бінарні або тернарні поліноми. Бінарні повинні мати d_f та d_g одиниць відповідно, а тернарні d_f та d_g коефіцієнтів 1 і $d_f - 1$ та d_g коефіцієнтів -1 відповідно. Поліном f є особистим ключем і повинен мати мультиплікативні інверсії за двома модулями.

Особистий ключ h обчислюється так:

$$h = p(f_q^{-1} * g) \bmod q. \quad (1)$$

Для шифрування використовуються поліноми r та M . Ці поліноми мають невелику ширину. Спочатку повідомлення M конвертується у відображення повідомлення поліном m . Потім обчислюється криптограма як:

$$e = h * r + m \bmod q. \quad (2)$$

Розшифрування здійснюється способом згортки поліномів у кільці як:

$$a = f * e \bmod q. \quad (3)$$

Після цього відбувається центрування коефіцієнтів поліному a . Для стандарту [1] коефіцієнти зводяться в інтервал $[-1024, 1024)$.

Вихідне відображення повідомлення (m) обчислюється як:

$$m = f_p^{-1} * a \bmod p. \quad (4)$$

2. СУТНІСТЬ ПОМИЛОК В ХОДІ РОЗШИФРУВАННЯ

Перепишемо формулу (3) у вигляді:

$$\begin{aligned} a &= f * e = f * (r * h + m) = \\ &= p * r * g + f * m \bmod q. \end{aligned} \quad (5)$$

Поліноми p, r, g, m, f обираються такими, що мають невелику ширину. В цьому випадку із дуже високою ймовірністю поліном $p * r * g + f * m$ матиме ширину меншу за q , що робить можливою редукцію в діапазоні $[A, A + q - 1]$, тобто порівняння за модулем q . Нагадаємо, що для [1] $A = -1024$. Якщо неправильно обрано загальносистемний параметр A , що відповідає за центрування коефіцієнтів (тоді деякі з коефіцієнтів $p * r * g + f * m$ лежатимуть за межами центрувального діапазону) або коли поліном $p * r * g + f * m$ матиме ширину більшу за q . У цьому випадку відновлене m' відрізнятиметься від вихідного повідомлення m на деякий множник числа q за модулем p . Це викличе помилки при розшифруванні, які можуть розкрити деяку інформацію про особистий ключ.

Існує два типи помилок розшифрування: wrapfailure («помилка обгортання») та gapfailure («помилка великого розриву»). Gapfailure виникає, коли $Width(p * r * g + f * m) \geq q$. Якщо ж $Width(p * r * g + f * m) < q$, але в процесі розшифрування через неправильний вибір A ми отримали помилку (неправильно обрано діапазон дозволених значень коефіцієнтів), то має місце помилка типу «wrap failure».

3. МОДЕЛЬ АТАКИ НА ОСНОВІ ПОМИЛОК РОЗШИФРУВАННЯ

3.1. Модель порушника

В даній атаці порушнику необхідно зібрати велику кількість триплетів (m, r, e) , де e — дійсна криптограма, отримана з відображення повідомлення m з використанням ключа сеансу r .

Тобто, порушник може проводити пасивну атаку просто прослуховуючи канал зв'язку і збираючи триплети або самостійно відправляти повідомлення і аналізувати криптограми.

3.2. Реверсивне представлення полінома

Позначимо зворотний до c поліном як $\bar{c}(X)$. Якщо $c = [c_0, c_1, c_2, \dots, c_{N-1}]$, то зворотний поліном має вигляд $\bar{c} = [c_0, c_{N-1}, c_{N-2}, \dots, c_1]$. Відображення $c \rightarrow \bar{c}$ є автоморфізмом кільця R , таким чином, застосування відображення двічі дає вихідний поліном c .

Таблиця 1

Дослідження бінарних та тернарних поліномів

Ітерація	Бінарний поліном		Тернарний поліном	
	$Width(u_i, \hat{f}_i)$	$Avr(u_i, \hat{f}_i)$	$Width(u_i, \hat{f}_i)$	$Avr(u_i, \hat{f}_i)$
1	29	9.83	19	7.28
2	24	9.69	18	7.1
5	24	9.66	18	6.82
10	23	9.45	17	6.09
100	22	9.45	16	5.68
1000	22	9.44	15	5.67

Позначимо добуток поліномів $c \cdot \bar{c}$ як $\hat{c}$. Цей добуток має властивість $\hat{c}_i = c \cdot (X^i * c)$, тобто кожний наступний терм полінома $\hat{c}$ отримується шляхом звичайного множення полінома c на свій зсув (ротацію). Відомо, що $\hat{c}_0 = \sum_i c_i^2 = \|c\|^2$, тоді як всі інші терми матимуть довжину приблизно $\|c\|$.

Таким чином, $f * \bar{f}$ має один терм довжини d_f , а всі інші — довжини $\sqrt{d_f}$. Якщо $p * r * g + f * m$ має достатньо велику ширину, це означає, що r значно корелює із $\bar{g}$, а m — із $\bar{f}$.

3.3. Сутність атаки

Загальна атака працює незалежно від використаної схеми доповнення відкритого тексту і використовує лише дійсні криптограми за рахунок повноцінних операцій.

Оскільки, поточна версія алгоритму NTRU вважається стійкою до помилок розшифрування і їх ймовірність складає 2^{-100} , реалізувати повноцінну атаку детектуючи помилки типу «garfailure» за допомогою оракула O_q фактично неможливо. Тому використовується оракул O_B , який визначає, чи є ширина полінома $p * r * g + f * m$ більша за B , де B можна обирати достатньо близьким до q (в залежності від кількості триплетів, якими володіє порушник).

Алгоритм атаки:

1. Встановити $u, v = 0$.
2. Згенерувати велику кількість дійсних криптограм $e = h * r + m \bmod q$. Для кожного шифротексту:
 - (а) Викликати $O_B(e)$.
 - (б) Якщо $O_B(e)$ показує, що ширина більша за B , встановити $u = u + \hat{m}$, $v = v + \hat{r}$.
3. Розділити u та v на кількість використаних криптограм.

При достатньо великій кількості помилок розшифрування u та v мають наблизитися до $\hat{f}$ та $\hat{g}$ відповідно.

4. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ НА ОСНОВІ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

Для практичних досліджень для тернарних поліномів використовувався набір параметрів ees401ep1: $N = 401$, $q = 2048$, $p = 3$, $d_f = 113$;

Позначимо $Width(u_i, \hat{f}_i)$ як найбільшу різницю між коефіцієнтами поліномів u та $\hat{f}$ на однакових позиціях та $Avr(u_i, \hat{f}_i)$ як середнє арифметичне усіх коефіцієнтів на однакових позиціях.

Звернемо вашу увагу, що у роботі [2] пропонується зворотний до $c = [c_0, c_1, c_2, \dots, c_{N-1}]$ поліном подавати у вигляді $\bar{c} = [c_0, c_{N-1}, c_{N-2}, \dots, c_1]$. У ході реалізації було встановлено, що краща кореляція буде при поданні зворотного полінома як $\bar{c} = [c_{N-1}, c_{N-2}, \dots, c_1, c_0]$, але для цього випадку потрібен буде інший алгоритм встановлення особистого ключа f з $\hat{f} = f * \bar{f}$, ніж зазначений у [4].

Обробка однієї криптограми, тобто один цикл алгоритму, залежить від швидкості шифрування криптосистеми (якщо порушник знаходиться у режимі очікування). Проте, якщо порушник назбирав велику кількість триплетів, то йому не складе зусиль обробити їх за досить невеликий час (один цикл алгоритму виконується приблизно за 1 мс).

Далі порушник може викрити особистий ключ f , використовуючи поліноміальний алгоритм, запропонований у [4]. Оскільки, отримане значення f є лише наближенням до дійсного, порушник може перебирати значення коефіцієнтів f зі значно меншого інтервалу та (або) виконати такі кроки:

1. Отримати значення v , яке є наближенням до $\hat{g}$. Згідно з алгоритмом атаки цей крок виконується паралельно з обчисленням u . Так, наприклад, на 1000-й ітерації для бінарних поліномів $Width(u_i, \hat{f}_i) = 27$, $Avr(u_i, \hat{f}_i) \approx 12$. А для тернарних: $Width(u_i, \hat{f}_i) = 18$, $Avr(u_i, \hat{f}_i) \approx 4$.

2. З формули (1) обчислення відкритого ключа маємо:

$$f * h = pg \bmod q. \quad (6)$$

Маючи відкритий ключ h та малий модуль p , порушник може змінювати коефіцієнти полінома f до отримання бінарного або тернарного полінома g використовуючи отримані наближення. Під час знаходження такого поліному його потрібно розглядати як претендента.

ВИСНОВОК

Хоча помилки під час розшифрування і не становлять суттєвої загрози на переглянуду версію NTRU (ймовірність такої помилки складає 2^{-100}), на їхній основі можна будувати досить успішні атаки. Це можливо за рахунок наявності кореляційних зв'язків поліномів та наближення ширини поліномів до значення великого модуля q , що й було використано у розглянутій моделі атаки.

Література

- [1] ANSI X9.98-2010. Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry.
- [2] N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman, A. Singer, and W. White. The impact of decryption failures on the security of NTRU encryption.

- [3] Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Монографія. Вид. 2-ге, перероб. і доп. — Харків: Видавництво «Форт», 2012. — 880 с.
- [4] C. Gentry, M. Szydlo. Cryptanalysis of the Revised NTRU Signature Scheme in Eurocrypt '02, LNCS 2332, pages 299–320 Springer-Verlag, Berlin, 2002.

Надійшла до редколегії 27.06.2014



Погребняк Костянтин Анатолійович, доцент кафедри БІТ ХНУРЕ, начальник відділу КЗІ АТ «ІІТ». Наукові інтереси: застосування методів алгебраїчної геометрії в криптології, асиметричний криптоаналіз.



Денисов Денис Сергійович, студент III-го курсу ХНУРЕ напряму БІКС. Наукові інтереси: асиметричні криптосистеми.

УДК 004.056.55

Общая атака на NTRUENCRYPT на основе ошибок расшифрования / К.А. Погребняк, Д.С. Денисов // Прикладная радиоэлектроника: науч.-техн. журнал. — 2014. — Том 13. — № 3. — С. 298–300.

NTRUEncrypt — это криптографическая система с открытым ключом, которая была создана в качестве альтернативы RSA и криптосистемам на эллиптических кривых (ECC). Исключительными особенностями NTRU являются оригинальный специфический математический аппарат и высокая скорость преобразований. Использование NTRU возможно при условии, что не существует криптоаналитических атак, которые могли бы существенно понизить ее криптографическую стойкость. Цель этой статьи — анализ защищенности криптосистемы от общей атаки на основе ошибок расшифрования.

Ключевые слова: NTRU, ошибки при расшифровании, общая атака на основе ошибок расшифрования.

Табл.: 01. Библиогр.: 04 назв.

UDK 004.056.55

General attack against NTRUEncrypt based on decryption failures / K.A. Pogrebnyak, D.S. Denisov// Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 298–300.

The NTRUEncrypt is a public key cryptosystem that has been developed as an alternative to RSA and ECC. NTRU is characterized by such features as specific background mathematics and high speed of transformations. The application of NTRU is possible if there are no cryptanalytical attacks which can substantially decrease its security. The aim of this paper is to analyze the cryptosystem security against a general attack based on decryption failures.

Keywords: NTRU, decryption failures, general attack based on decryption failures.

Tab.: 01. Ref.: 04 items.

ПРИМЕНЕНИЕ КОДОВ АУТЕНТИФИКАЦИИ СООБЩЕНИЙ ДЛЯ ОБНАРУЖЕНИЯ МОДИФИКАЦИЙ ДАННЫХ В РЕГИОНАЛЬНЫХ СИСТЕМАХ ДИФФЕРЕНЦИАЛЬНОЙ КОРРЕКЦИИ НАВИГАЦИОННЫХ СИГНАЛОВ СИСТЕМ GPS/ГЛОНАСС

Т.А. ГРИНЕНКО, А.П. НАРЕЖНИЙ

В данной статье обосновывается необходимость применения кодов аутентификации сообщений (МАС) для обеспечения целостности и достоверности корректирующей информации, формируемой системами дифференциальной коррекции навигационных сигналов систем GPS/ГЛОНАСС. На примере работы типовой схемы контрольно-корректирующей станции обосновывается необходимость применения МАС — алгоритмов при передаче «сырых» измерений уточненных эфемерид и частотно-временных поправок навигационно-космических аппаратов глобальных навигационных спутниковых систем GPS/ГЛОНАСС.

Ключевые слова: контрольно-корректирующая станция, защита данных, криптография, коды аутентификации сообщений.

ВВЕДЕНИЕ

Постановка проблемы. Современная система координатно-временного и навигационного обеспечения Украины строится на использовании радионавигационного поля глобальных навигационных спутниковых систем (ГНСС) GPS (США) и ГЛОНАСС (Российская Федерация), а также корректирующей информации (КИ) Европейской спутниковой системы дифференциальной коррекции (СДК) типа EGNOS (European Geostationary Navigation Overlay Service) [1]. Вместе с тем владельцами ГНСС являются военные ведомства данных стран, которые не исключают введение селективного доступа (Selective Availability, SA) к радионавигационным сигналам. Для повышения точности позиционирования и устранения влияния режима SA в мире строятся различные СДК. Поэтому для решения целого ряда задач экономики, безопасности и обороны в Украине разрабатывается ряд проектов, направленных на построение национальной СДК радионавигационных сигналов GPS/ГЛОНАСС [2].

Обеспечение аутентичности КИ радионавигационного поля ГНСС является одной из основных проблем, которые возникают перед разработчиками современных автоматизированных СДК. Актуальной эта проблема стала и для разработчиков функционального дополнения ГЛОНАСС в рамках развития проекта российской системы дифференциальной коррекции и мониторинга [3]. В результате был разработан Национальный стандарт Российской Федерации ГОСТ Р 54459-2011, который описывает общетехнические требования к СДК и обязывает разработчиков применять в аппаратно-программных комплексах данной системы средства защиты информации, передаваемой по общедоступным каналам связи [4].

Анализ литературы. В конце 2012 года исследователи из Университета Карнеги-Меллон

и компании Coherent Navigation классифицировали новые типы уязвимостей системы GPS и оценили масштаб связанных с ними угроз [5]. В работе [5] описано несколько техник атаки на инфраструктуру системы GPS. Эта атака отличается от традиционных методов джамминга и спуфинга большим масштабом и представлением информационной системы GPS как компьютерной сети. В эксперименте по тестированию нового метода спуфинга были задействованы контрольные сообщения протокола GPS (в первом методе), особенности программного стека GPS (во втором методе) и программного обеспечения GPS-приёмников (третий метод).

Используя относительно простую аппаратно-программную систему, собранную из доступных на рынке недорогих элементов, эти специалисты провели несколько новых концептуальных атак на GPS-устройства. При этом применялись следующие приёмы: фальсификация эфемерид GPS-спутников; передача некорректной информации о текущей дате; намеренная рассинхронизация шкал времени (ШВ); атака на системное программное обеспечение устройства (вторжение, повышение привилегий в системе); дезориентирующее искажение сигнала — псевдослучайного кода (спуфинг).

Атака апробирована на GPS-приёмниках семи производителей, включая Magellan, Garmin, GlobalSat, uBlox, LOCOSYS и iFly 700. Подобные устройства используются в легковых и грузовых автомобилях, самолётах, беспилотных летательных аппаратах, кораблях, станциях сотовой связи, в системах диспетчерского управления и сбора данных типа SCADA (Supervisory Control And Data Acquisition) и т.д. [6,7].

Кроме того, в работе [5] показано, что в результате 45-секундной сессии можно вывести из строя до 30% станций CORS (Continuously Operating Reference Stations) системы GPS и до 20% сетей, использующих протокол NTRIP

(Networked Transport of RTCM via Internet Protocol) [8].

Сеть станций CORS является аналогом региональной СДК, т. к. используется для ретрансляции данных ГНСС преимущественно на территории США, а сети с протоколом NTRIP передают данные системы GPS в онлайн. Исследователи показали, что многие коммерческие GPS-приёмники полагаются на эти данные, но из-за отсутствия криптографических методов проверки подлинности GPS-пакетов в коммерческих приложениях эти GPS-приёмники уязвимы к атакам. Для GPS-приёмников военного назначения, в которых используется криптографическая защита передаваемых данных, предлагаемый метод атаки [5] не работает.

На международной конференции ZeroNights 2012 года участник конференции, кандидат наук по безопасности встроенных устройств из университета EURECOM, Андрей Костин сообщил об уязвимости GPS системы наблюдения воздушного потока, экспериментально подтвердив возможность модифицировать данные сигналов протокола ADS-B (система наблюдения воздушного потока, которую диспетчеры и пилоты используют для отслеживания местонахождения самолетов, а также передачи важных данных и параметров). Как оказалось, протокол не использует никаких средств защиты при передаче данных, например, шифрования или электронной цифровой подписи [9]. Это позволяет отслеживать все самолеты в режиме реального времени и, самое главное, посылать в эфир поддельные данные или подменивать данные в настоящих пакетах, чтобы, например, симитировать на экранах контролеров полетов воздушное столкновение самолетов.

Известно [10], что в среде Internet КИ от контрольно-корректирующей станции в СДК к потребителям в реальном времени доставляется в формате RTCM SC-104 (версия 2.2 и выше). Для этого применяют два протокола: SISNet и NTRIP [11]. Например, SISNet используют для распространения КИ, формируемой системой EGNOS. Протокол NTRIP применяют в функциональном дополнении ГНСС ГЛОНАСС – Российской системы дифференциальной коррекции и мониторинга [4, 12].

Перехват и модификация КИ в формате RTCM в Internet среде начинает принимать массовый характер. Согласно исследованиям [6, 7], информация с недорогих встроенных в смартфон устройств геопозиционирования или персональных GPS-устройств, отслеживающих местонахождение потребителя, может с лёгкостью быть перехвачена хакерами, которые потом могут точно определить местонахождение устройства, выдать его за другой объект или подделать информацию о его физическом местонахождении.

Между тем, принято считать, что вероятность хакерской атаки на локальные ККС из состава

национальной системы СДК незначительна, т. к. для реализации атаки необходимо применять дорогостоящие эталонные комплексы. Вследствие этого в Украине при разработке проектов региональных и ведомственных СДК вопросы защиты информации не рассматриваются. Наряду с этим не учитывается, что для обеспечения информационного взаимодействия в СДК будет использоваться Internet, т. к. в стране отсутствуют национальные системы передачи КИ [11].

В настоящее время вся информация о «сырых» измерениях уточненных эфемерид и часотно-временных поправок навигационного космического аппарата (НКА) систем GPS/ГЛОНАСС, полученная национальными ККС, передается в открытом виде. Вследствие этого существует реальная опасность хакерских атак на локальные ККС из состава национальной СДК. Поэтому применение криптографической защиты данных в СДК с целью повышения их стойкости и надежности является актуальной научно-технической задачей.

Цель статьи. Обоснование необходимости применения MAC кодов для обеспечения целостности и достоверности КИ в национальной СДК ГНСС GPS/ГЛОНАСС. Предлагается использовать MAC коды для выявления несанкционированных модификаций «сырых» данных, передаваемых пользователям ГНСС, как в зоне отдельно действующего пункта контроля, так и в зоне действия всей СДК в целом.

ОСНОВНАЯ ЧАСТЬ

Дифференциальный режим измерений основывается на пространственно-временной корреляции основных погрешностей измерений в навигационной аппаратуре потребителей (НАП) и в опорной точке Земной поверхности, где устанавливается контрольно-корректирующая станция (ККС). Математическая постановка задачи дифференциального режима измерений состоит в следующем. Вектор состояния ККС в общем случае имеет следующий вид

$$\vec{\lambda}_k = [x, y, z, \Delta T_k, \Delta_{0f_k}]^T,$$

где (x, y, z) – точные координаты локальной (мобильной) ККС в системах геодезических параметров Земли ПЗ-90 или WGS-84; ΔT_k – отклонение ШВ системы GPS от национальной координированной шкалы UTC(UA) в k -й момент времени передачи КИ; Δ_{0f_k} – относительное отклонение частоты опорного генератора в k -й момент времени передачи КИ.

Погрешность определения координат для ККС задается следующими соотношениями:

$$\Delta x_0 \in N(0, \sigma_{\Delta x}^2), \Delta y_0 \in N(0, \sigma_{\Delta y}^2), \Delta z_0 \in N(0, \sigma_{\Delta z}^2),$$

где $N(0, \sigma_{\Delta z}^2)$ – нормальный закон распределения величины $\Delta z_0 = z - z_0$, с нулевым математическим ожиданием и дисперсией $\sigma_{\Delta z}^2$ привязки к точному значению координаты z_0 фазового центра антенны НАП в системе координат WGS-84.

При этом уравнение состояния шкалы ККС в k -й момент передачи КИ, будет иметь вид

$$\Delta T_k = \Delta T_{k-1} + \left[1 - e^{-\alpha \Delta t}\right] \alpha^{-1} \frac{\Delta f_{k-1}}{f_0} + \xi_{\Delta T, k-1}, \quad (1)$$

где $\alpha \approx 0.1$ Гц — характеризует ширину энергетического спектра эталонного сигнала времени системы GPS, а $\Delta t = t_{k+1} - t_k$; $f_0 = 1.5 \cdot 10^9$ Гц — номинальное значение аналитической частоты сигнала L1 системы GPS; $\xi_{\Delta T, k-1}$ — гауссовский процесс типа белого шума с математическим ожиданием: $M[\xi_{\Delta f, k}] = 0$ и корреляционной функцией: $M[\xi_{\Delta f, k+1} \xi_{\Delta f, k}] = R_\xi \delta(\Delta t)$; Δf_{k-1} — частотные флуктуации сигнала системы GPS относительно эталонной частоты ККС.

Частотные флуктуации радионавигационного сигнала системы GPS задаются стационарным марковским процессом первого порядка с корреляционной функцией вида: $R_{\Delta f}(\Delta t) = \sigma_{\Delta f}^2 e^{-\alpha |\Delta t|}$, где $\sigma_{\Delta f}^2 \approx 0.25$ Гц² — мощность частотных флуктуаций сигнала системы GPS.

Корреляционные интегралы, формируемые в корреляторе НАП, позволяют отследить модуляцию сигнала НКА символами информации и вычислить метку времени во входном сигнале. Метки времени следуют с периодичностью 6 с для GPS. В пределах одного деления этой шкалы периоды дальномерного кода образуют 1 мс шкалу. Одна миллисекунда разделена в свою очередь на отдельные элементы для GPS — 1023 элемента. Потому в НАП относительное отклонение частоты опорного генератора представляется в виде разности метки времени, сформированной собственным генератором, и системной метки времени GPS, и выражается в мс. Получить относительное отклонение частоты опорного генератора НАП можно из соотношения

$$\Delta_{0f_k} = \frac{\Delta f_k}{f_0} = -\frac{\Delta t_k / \tau_\Sigma}{1 + \Delta t_k / \tau_\Sigma},$$

где Δt_k — разность меток времени в мс, переданных НАП в k -й момент времени; а τ_Σ — длительность элементарного символа псевдослучайной последовательности дальномерного C/A-кода системы GPS ($\tau_\Sigma \approx 1$ мкс).

Намеренное искажение данных вектора состояния ККС является основной задачей кибератаки. Данный тип хакерской атаки относится к типу атак модификации [5]. Стандарты RTCM SC-104 определяют сообщения, которые содержат информацию о референцной станции (или ККС) и системные данные. Используя концепцию виртуальной референцной станций (Virtual Reference Station, VRS) [13] и внося ошибки в вычисления поправки в псевдодальности для каждой ККС, можно значительно исказить информацию потребителя о его истинном местоположении. Протокол NTRIP может быть использован для передачи RTCM данных для VRS. Корректирующая информация RTCM получается для виртуальной точки, соответ-

ствующей примерному местоположению пользователя, на основании данных с некоторого количества референцных станций (или ККС).

Таким образом, наиболее просто можно осуществить атаку на ККС путем создание VRS. Для этого необходимо осуществить следующую схему атаки:

1. Произвести идентификацию координатных, частотно-временных параметров ККС и осуществить их модификацию при передаче по сети Internet.

2. Произвести постановку помехи и блокировать ГНСС приемники ККС.

3. Осуществить эмуляцию «сырых» данных с заблокированной ККС для не обнаружения модификации данных для пользователей локальной ККС при обработке их в центре сбора данных СДК.

Для осуществления успешной атаки необходимо знать метрологические характеристики аппаратуры: НАП и опорной квантовой меры частоты (КМЧ). При этом с учётом частотно-временных погрешностей, вносимых НАП, изменения относительного отклонения частоты Δ_{0f_k} опорного генератора ККС должно определяться с погрешностью на суточном интервале наблюдения менее $1 \cdot 10^{-13}$. Кроме того, необходимо знать оценку погрешности расхождения шкал времени ККС относительно НКА и координированной шкалы UTC(UA). Пределы допускаемой погрешности измерения расхождения внутренней ШВ ККС относительно координированной шкалы UTC(UA) $\leq \pm 10$ нс.

Предел допускаемой погрешности формирования дифференциальных поправок в формате RTCM SC-104, версия 2.2 (при доверительной вероятности 0,99) равен ± 0.3 м. Поэтому средняя квадратическая погрешность взаимной геодезической привязки координат (x, y, z) локальных (мобильных) ККС национальной СДК в системах геодезических параметров Земли ПЗ-90 или WGS-84 должна быть не более 0.1 м.

В настоящее время данные параметры (вектор состояния) получают на основании измерений с помощью дорогостоящих эталонных комплексов. Поэтому практическую апробацию атаки модификации вектора состояния ККС произведем на основе перехвата данных «сырых» измерений частотно-временных поправок кодовых наблюдений C/A кода на несущей частоте L1 навигационного сигнала GPS, принимаемого НАП. При этом атака модификации должна производиться в два этапа.

На первом этапе производится оценка суммарной погрешности навигационного сигнала GPS: погрешности, относящейся к НКА; погрешности, относящейся к НАП; погрешности, относящейся к среде распространения радиоволн [14]. Информация для первого этапа может быть получена из открытых источников и специализированных сайтов.

На втором этапе производится определение:

а) ковариационной матрицы результатов измерения ККС;

б) относительного отклонения частоты $\Delta_0 f_k$ опорной КМЧ из состава ККС;

в) оценки поправки $t = t_c + \Delta t_c$ к ШВ опорной КМЧ из состава ККС:

$$\Delta t_c = a_0 + a_1(t_c - t_{oc}) + a_2(t_c - t_{oc})^2,$$

где a_0, a_1, a_2 — коэффициенты, передаваемые ККС в центр управления национальной СДК; t_c — время, передаваемое ККС; t_{oc} — опорное время блока временных данных, измеренное от начала еженедельной временной программы системы GPS.

Для второго этапа предлагается методика экспериментальной оценки вектора состояния ККС с помощью навигационного сигнала GPS, при использовании в качестве опорных генераторов рубидиевых КМЧ с оптической накачкой типа СЧВ-73, СЧВ-74. Выбор данного типа КМЧ обусловлен тем, что они широко используются в качестве высокостабильных источников сигналов для проверки опорных генераторов частотно-временной аппаратуры различных потребителей Украины, а также для хранения ШВ на образцах вооружения и военной техники. Кроме того, в методике учитывается, что в Украине широко распространена только одночастотная НАП, поэтому применяются алгоритмы, использующие только измерения С/А кода на несущей частоте L1 (1575,42 МГц) навигационного сигнала GPS.

В качестве НАП сигналов GPS/ГЛОНАСС предлагается использовать серийную аппаратуру национального производителя ГП „Оризон-Навигация” (г. Смела, серия СН). Например, устройство временной синхронизации с использованием сигналов GPS/ГЛОНАСС "Navio-S" (СН-3834) [15]. Данный НАП представляет собой 14-канальный специализированный приемник, работающий по сигналам спутников GPS/ГЛОНАСС, используя С/А и ПТ коды на несущей частоте L1. Сопряжение с ПЭВМ осуществляется по последовательным интерфейсам RS-232, с возможностью обмена информацией по протоколам NMEA 0183 (расширенный протокол), BINR (фирменный протокол «КБ НАВИС») и RTCM SC-104 v2.2 [10, 13, 16]. Кроме того, конструкция НАП типа СН-3834 позволяет в качестве опорного генератора использовать внешний генератор, что позволяет реализовать метод внешней синхронизации. Это необходимо для уменьшения влияния нестабильности частоты внутреннего опорного кварцевого генератора СН-3834 на результаты измерений ККС.

ЭКСПЕРИМЕНТАЛЬНАЯ ЧАСТЬ

Для осуществления кибератаки необходимо наряду с программными средствами применять и аппаратные средства. При этом минимально необходимые аппаратные средства, имитирую-

щие работу стационарной ККС приведены на рис. 1. На схеме приемник СН-3834 синхронизируется сигналом опорной КМЧ частотой 5 МГц. Радионавигационные сигналы, принятые антенной, поступают на антенный вход СН-3834, с выхода которого сигнал "1PPS" (аппаратная метка времени) подается на вход "Б" частотомера типа ЧЗ-64/1. Секундная метка от опорного генератора СЧВ-74 подается на вход "А" частотомера ЧЗ-64/1. При этом частотомер работает в режиме измерения интервалов времени. Информация с выхода частотомера ЧЗ-64/1 через интерфейс IEEE488 передается в ПЭВМ для дальнейшей обработки и хранения. ПЭВМ оборудована платой контроллера интерфейса IEEE 488 (канала общего пользования ГОСТ 26.003-80), имеющую программную поддержку в стандарте VISA Revision 3.0.

Таким образом, с помощью частотомера ЧЗ-64/1 измеряется интервал времени, который соответствует размеру фазового сдвига между двумя этими сигналами, т.е. равняется времени задержки эталонного сигнала времени, который передается в составе навигационного сигнала, относительно системной ШВ ККС, формируемой СЧВ-74. Для хранения координированной шкалы UTC (UA) применяется синхрометр типа Ч7-37, который осуществляет привязку КИ в ККС и выдает в ПЭВМ через интерфейс IEEE488 информацию о коде текущего значения времени. Для усиления эталонных сигналов 5 МГц в ККС применяется усилитель высокочастотный распределительный типа ЯЗЧ-74.

При проведении эксперимента соблюдались нормальные климатические условия. Время наблюдения $\tau_n = 21970$ с, интервал времени измерения $\tau_i = 1$ с, темп выборки $\tau_b = \tau_i$. Информация о параметрах ШВ приемника была получена по СОМ-порту в протоколе BINR. Для работы с фирменным протоколом BINR на языке Borland C++ Builder 6.0 было разработано специализированное программное обеспечение, позволяющее через интерфейс RS232 осуществлять доступ к «сырым» измерениям частотно-временных поправок кодовых наблюдений С/А. Для этого в НАП посылался запросный пакет 1f. Ответный пакет №72 протокола BINR содержит информацию о времени. При этом учитывалось, что пакет №72 передается с опережением на 300–400 мс относительно выходного импульса 1PPS. Данные, выдаваемые ответным пакетом №72 (данные о частоте и времени) протокола обмена BINR: текущее относительное отклонение частоты опорного генератора с точностью $1 \cdot 10^{-10}$ и текущее отклонение меток времени от шкалы UTC (нс).

Необходимо также получать данные, выдаваемые ответным пакетом №84 (последнее решение) протокола обмена BINR: широта (радианы), долгота (радианы), высота (метры), время определения (мс), среднее квадратичное отклонение (СКО) координат (метры).

Задержка сигнала в тракте от антенны до измерителя временного интервала в НАП компенсируется за счет соответствующей калибровки приемника.

При помощи программного обеспечения «сырые» данные НАП СН-3834 преобразовываются в КИ и в формате RTCM SC-104 посылаются на сервер NTRIP. В задачу сервера входило распространение КИ посредством сети Internet. В ходе эксперимента вырабатывалась и доставлялась потребителю КИ, содержащая поправки только к кодовым измерениям (кадры RTCM SC-104 № 1, 31).

Данные о сдвиге шкалы ΔT , переданные в составе частотно-временного пакета № 72 протокола BINR и обрабатываемые с помощью разработанного программного обеспечения, приведены на рис. 2.

Из анализа данных следует, что если абсолютное значение разности между измеренной в приемнике и расчетной ШВ превышает порог 12 нс, то приемник делает сдвиг своей ШВ на 12 нс соответственно вперед или назад во времени. Некомпенсированный остаток от разности указанных ШВ округляется до одной наносекунды и передается в составе частотно-часового пакета № 72 протокола BINR. Отсюда следует, что погрешность измерения значения кода фазы (code

phase) соответственно равна $\tau_{\phi}/N_{\text{КВ}} \approx 0.98$ нс, где $N_{\text{КВ}} = 2^{10}$ — число, определяемое схемой слежения СН-3834 за задержкой огибающей сигнала.

При этом погрешность формирования сигнала на выходе 1PPS в режиме слежения за НКА становится не более 25 нс. Таким образом, обеспечивается стабильность воспроизведения приемником СН-3834 меток времени UTC с погрешностью ± 12 нс.

Выделяя в данной последовательности чисел 12 нс скачки фазы и компенсируя их получим последовательность, представленную на рис. 3. Применяя метод наименьших квадратов, определим в данной последовательности линейную функцию ухода ШВ опорной КМЧ вида

$$T(t_k) = \Delta_{0f_k} t_k + T_0, \quad (2)$$

где T_0 — разность шкалы КМЧ и системной шкалы GPS, соответствующая начальному моменту времени t_0 .

При этом гистограмма и плотность вероятности невязок ШВ относительно $T(t_k)$ будет иметь вид, представленный на рис. 4.

Для описания статистической модели невязок значений ШВ было взято семейство распределений с плотностью вероятности вида:

$$f(\Delta T_k, m_i, \sigma_i, \kappa_i, I) = \sum_{i=1}^I \left[\frac{\kappa_i}{\sigma_i \sqrt{2\pi}} \exp \left(-\frac{\Delta T_k - m_i}{2\sigma_i^2} \right) \right],$$

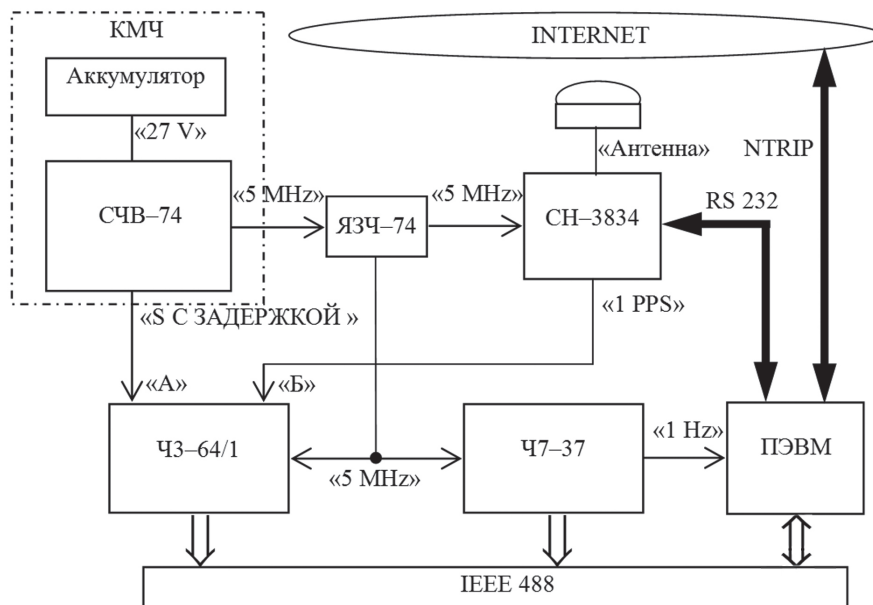


Рис. 1. Функциональная схема стационарной ККС с опорной КМЧ типа СЧВ-74

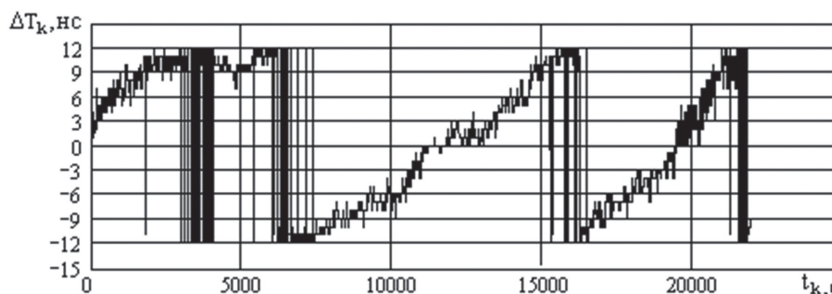


Рис. 2. График «сырых» данных результатов сличения поправок ШВ, переданных в составе частотно-временного пакета № 72 протокола BINR

где $m_i, \sigma_i^2, \kappa_i$ — математическое ожидание, дисперсия, нормировочный коэффициент i -й плотности нормального распределения, а параметр $I = 3$.

Поиск неизвестных параметров $m_i, \sigma_i^2, \kappa_i$ данного распределения проводился методом наименьших квадратов [17]. Проверка гипотезы о законе распределения проводилась с использованием критерия согласия «хи-квадрат».

Найденные плотности распределения невязок значений ШВ для ККС изображены на рис. 4 штрих пунктиром.

В данном случае относительного отклонения частоты опорного генератора $\Delta_{0fk} = 2.5 \cdot 10^{-12}$. При этом СКО значений Δt от линейной функции составляет 4.2 нс.

Доверительный интервал определения относительного отклонения действительного значения частоты от своего номинального значения на суточном интервале наблюдения при таком значении СКО составляет $1.5 \cdot 10^{-13}$. Таким образом, использование уточняющей частотно-временной информации, переданной в составе пакета № 72 протокола BINR приемника СН-3834, позволяет, с одной стороны, уменьшить значение доверительного интервала определения действительного значения частоты КМЧ, а, с другой стороны, остается недостаточным для определения метрологических характеристик прецизионных КМЧ из состава ККС. Это приводит к необходимости поиска алгоритмов дополнительной компенсации флуктуаций меток времени, переданных НАП типа СН-3834, с целью их использования для оценки относительного отклонения действительного значения частоты Δ_{0f} опорного генератора ККС с погрешностью на суточном интервале наблюдения $\leq 1 \cdot 10^{-13}$.

Приемник СН-3834 выделяет метки времени, переданные каждым НКА из числа рабочего созвездия, и измеряет интервалы времени между меткой времени своей собственной ШВ, сформированной внутренним опорным генератором (при внешней синхронизации — КМЧ, подключенным на вход внешней синхронизации) и метками времени, принятыми от каждого НКА. Данные интервалы времени используются как исходная информация для навигационной задачи определения координат ККС на основе разностно-дальномерного метода. Знание координат ККС разрешает определить дальность до каждого НКА из состава рабочего созвездия. Используя значение скорости распространения радиоволны, эти дальности могут быть пересчитаны в абсолютные значения задержек ШВ каждого НКА, обусловленных временем распространения сигнала от НАК до НАП. Поэтому погрешности определения координат ККС будут непосредственно входить в состав погрешности синхронизации шкалы ККС.

Определение интервала времени задержки системной ШВ в приемнике СН-3834 осуществляется путем расчета времени распространения от НКА, который находится в зените, относительно места положения фазового центра антенны. В этом случае влияние ионосферы на скорость распространения электромагнитной волны будет минимальным. Поэтому основной вклад в погрешность определения задержки будет вносить погрешность определения места положения фазового центра антенны приемника по высоте.

На рис. 5 приведены результаты определения места положения по высоте с помощью приемника типа СН-3834 для стационарной ККС, которые передаются в составе пакета № 84.

Если сравнить данные результатов определения местоположения ККС по высоте с резуль-

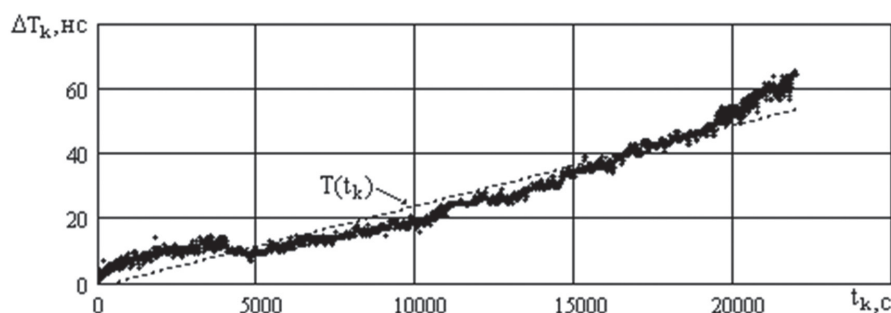


Рис. 3. График ухода ШВ после устранения неоднозначности значения кода фазы на несущей частоте

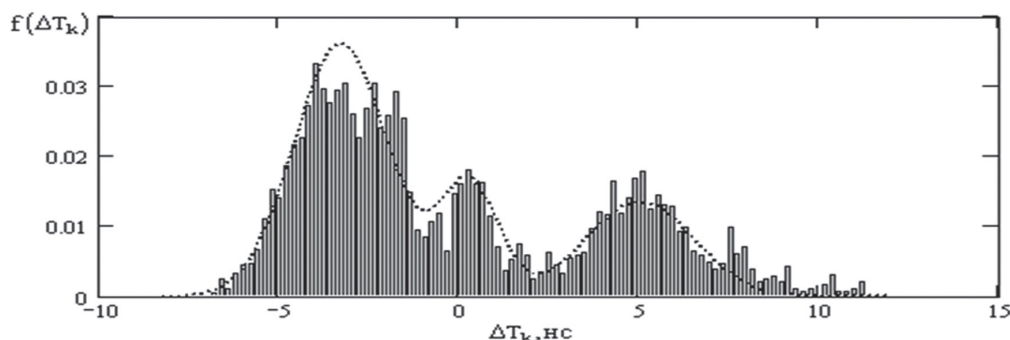


Рис. 4. Гистограмма и плотность вероятности измерений невязок ШВ

татами отклонений аппаратной метки времени приемника от аппроксимации линейной функций (приведенной на рис. 3), можно увидеть их качественное совпадение. Результаты сравнения приведены на рис. 6.

Количественной мерой степени связи двух случайных процессов есть коэффициент их взаимной корреляции, который рассчитывается по формуле

$$R_{h,\Delta\tau} = \frac{\frac{1}{N} \sum_{k=1}^N [h_k - M(h_k)][\Delta\tau_k - M(\Delta\tau_k)]}{\sqrt{D(h_k)D(\Delta\tau_k)}}, \quad (3)$$

где $N = \tau_H / \tau_B$ – количество наблюдений (объем выборки); $M(h_k) = \frac{1}{N} \sum_{k=1}^N h_k$ – оценка математического ожидания высоты потребителя над геоидом, полученная по результатам выборки последнего решения, представленного в пакете № 84 протокола BINR приемника СН-3834; $M(\Delta\tau_k) = \frac{1}{N} \sum_{k=1}^N \Delta\tau_k$ – оценка математического ожидания отклонения поправок к аппаратным меткам времени, сформированных в пакете № 72 протокола BINR приемника СН-3834, от линейной функции вида (2); $D(h_k) = \frac{1}{N} \sum_{k=1}^N [h_k - M(h_k)]^2$ – оценка дисперсии определения места положения над уровнем моря потребителя, полученная по результатам выборки последнего решения, представленного в пакете № 84 протокола BINR приемника СН-3834; $D(\Delta\tau_k) = \frac{1}{N} \sum_{k=1}^N [\Delta\tau_k - M(\Delta\tau_k)]^2$ – оценка дисперсии поправок к аппаратным меткам времени, сформированных в пакете № 72 протокола BINR приемника СН-3834, от линейной функции (2).

Для данной реализации значение $R_{h,\Delta\tau}$ равняется 0,8, что свидетельствует о наличии сильной связи между двумя случайными процессами. Это позволяет использовать информацию об отклонении определения места положения ККС по высоте от своего среднего значения с целью компенсации погрешности определения отклонения аппаратной ШВ приемника СН-3834 от координированной шкалы UTC (USNO).

С этой целью введем поправку к метке времени, сформированной в k -й момент времени

$$\delta\tau_k = m_t \Delta h_k, \quad (4)$$

где Δh_k – отклонение оценки места положения ККС по высоте от своего среднего значения, полученное в k -й момент времени; m_t – некоторый коэффициент пропорциональности, который разрешает согласовать размерности величин, которые входят в выражение (4) и оптимизировать вес данной поправки.

С учетом выражения (4), уточненное значение поправки ΔT , переданное в составе пакета № 72 протокола BINR приемника СН-3834, можно определить с помощью следующего соотношения

$$\Delta T_{y,k} = \Delta T_k - \delta\tau_k, \quad (5)$$

где ΔT_k – значение поправки к аппаратной ШВ приемника, переданное в составе пакета № 72 протокола BINR.

Коэффициент m_t , который входит в состав выражения (4), существенным образом влияет на количественное значение оценки погрешности задержки ШВ, обусловленной погрешностью определения места положения ККС. Поэтому естественной является его оптимизация.

Оптимизацию коэффициента m_t целесообразно проводить на основе минимизации отклонения поправки $\Delta T_{y,k}$ от ее аппроксимации

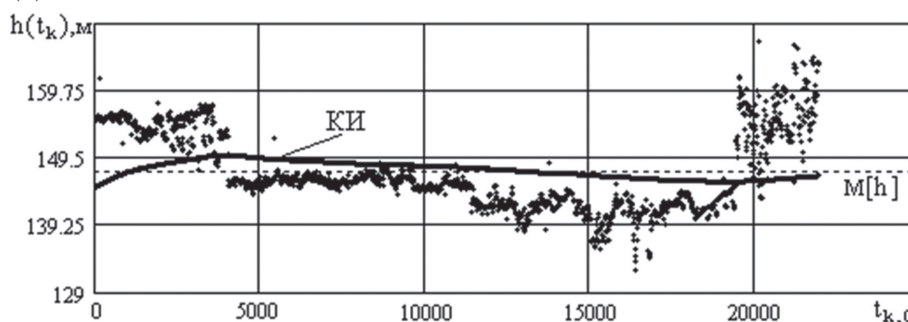


Рис. 5. Результаты определения местоположения ККС по высоте с помощью НАП типа СН-3834

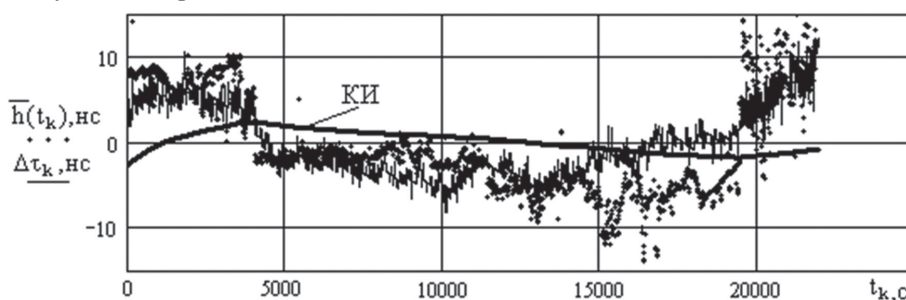


Рис. 6. Результаты сравнения определения местоположения ККС и отклонений аппаратной метки времени приемника от аппроксимации линейной функцией

линейной функцией вида (2), что представляет собой условное среднее значение отклонения аппаратной ШВ от шкалы UTC (USNO). Количественной оценкой отклонения случайного процесса от условного среднего есть его дисперсия вида

$$\sigma_{\Delta\tau}^2 = \frac{1}{N} \sum_{k=1}^N [\Delta T_{y,k} - T(t_k)]^2. \quad (6)$$

Зависимость СКО от величины коэффициента m_t приведена на рис. 7. Видно наличие явного минимума СКО в окрестности значения $m_t = 0.56$. При этом само значение СКО уменьшается от значения $17.2 \cdot 10^{-9}$ до значения $6.7 \cdot 10^{-9}$. Дальнейшее уменьшение значения среднего квадратичного отклонения $\sigma_{\Delta\tau}$ возможно путем применения цифрового рекурсивного фильтра [4]. Применим рекурсивный фильтр следующего вида

$$\Delta \bar{T}_k = (1 - \alpha) \Delta \bar{T}_{k-1} + \alpha [\Delta T_{y,k} - T(t_k)]. \quad (7)$$

Решение задачи синтеза рекурсивных фильтров сводится к нахождению коэффициента α . Известны прямые и косвенные методы синтеза рекурсивных фильтров [3, 17]. Прямые методы основаны на непосредственном определении параметров цифровых рекурсивных фильтров по заданным временным или частотным характеристикам. Косвенные методы синтеза рекурсивных фильтров основаны на дискретизации аналогового фильтра, удовлетворяющего заданным требованиям. Применяя косвенный метод синтеза рекурсивного фильтра, получим значение коэффициента $\alpha = 0.1$. Данный коэффициент позволяет фильтру устранить имеющиеся большие одиночные выбросы и существенным образом сгладить флуктуации поправки к аппаратной ШВ и соответственно уменьшить значение СКО и, в то же время, оставаться чувствительным к медленным вариациям поправки, обусловленным изменением частоты внешней синхронизирующей КМЧ.

Результат сглаживания приведен на рис. 8 штриховой линией. Сплошной линией приведены исходные результаты отклонения поправки к аппаратной ШВ от линейной аппроксимирующей функции вида (2).

СКО результирующей поправки от линейной аппроксимирующей функции составляет $2 \cdot 10^{-9}$ с, что позволяет уменьшить доверительный интер-

вал определения относительного отклонения частоты на суточном интервале наблюдения до значения $6 \cdot 10^{-14}$. Такое значение доверительного интервала уже есть приемлемым для получения достоверных оценок относительного отклонения действительного значения частоты КМЧ с необходимой точностью на основе анализа «сырых» данных, что эквивалентно сличению с более стабильными мерами частоты: водородными или цезиевыми КМЧ.

Таким образом, использование в обработке данных протокола №72 позволяет на порядок повысить точность определения относительного отклонения действительного значения частоты на суточном интервале наблюдения в сравнении с использованием аппаратной метки (с $2 \cdot 10^{-12}$ до $2 \cdot 10^{-13}$). При этом предлагаемый алгоритм компенсации погрешности формирования метки времени повышает точность определения оценки относительного отклонения действительного значения частоты опорного генератора вдвое, т.е. до $6 \cdot 10^{-14}$.

Оценка трёх координат в векторе состояния ККС в системе WGS-84 по данным выдаваемым пакетом №84 (последнее решение) протокола обмена BINR приемника СН-3834 имеет вид: $x = 3322269.4975$ м; $y = 2428959.4668$ м; $z = 4901486.0223$ м. Математическое ожидание $M[h]$ высоты фазового центра антенны НАП в системе WGS-84 равно 147.67 м. Сравним данную оценку высоты с эталонной, которая вычислена на основании данных стереотопографической съемки, полученной от Харьковского городского управления архитектуры. Так, значение нормальной высоты h_y фазового центра приемной антенны (ПКАН.434854.023) в местной системе координат равно 151.93 м. Однако высота h_{WGS-84} представляет собой геодезическую высоту: высоту точки земной поверхности над рассматриваемым эллипсоидом, отсчитанную по нормали к его поверхности. При этом высоты, полученные по материалам нивелирования земной поверхности и приводимые в геодезических каталогах и на топографических картах, относятся к системе нормальных высот, которая применяется в нашей стране. С учетом того, что нормальные высоты в Украине отсчитываются от поверхности квазигеоида Земли в Балтийской системе высот 1977 года, то геодезическая высота h_{WGS-84} определяется в виде

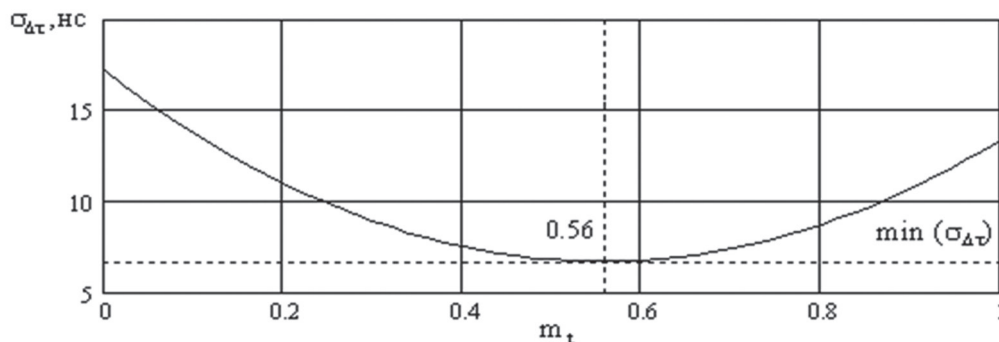


Рис. 7. Зависимость СКО ШВ от величины коэффициента m_t

$$h_{WGS-84} = h_y + \Delta h + \zeta,$$

где Δh — разность высот, которую можно определить через матричные преобразования системы ПЗ-90 в систему WGS-84 [2,3], ζ — аномалия высоты (превышение квазигеоида над эллипсоидом ПЗ-90). При этом погрешность от аномалии высоты для системы WGS-84 может лежать от 2 до 6 м [8]. Величина ζ связана с аномалией гравитационного поля и меняется в зависимости от координат и составляющих уклонений отвесной линии. В целом значения ζ для разных территорий Украины определены. Однако для общего земного эллипсоида ПЗ-90 и референц-эллипсоида Красовского они не совпадают.

Таким образом, используя два протокола из состава внутреннего программного обеспечения НАП типа СН-3834 возможно без применения эталонного оборудования оценить вектор состояния ККС с высокой точностью.

Модификация данных вектора состояний ККС при таком виде атаки позволит полностью захватить управление выдачи КИ в СДК. Для устранения данной угрозы необходимо применять процедуру аутентификации КИ в ККС, которая представляет собой процедуру проверки того, что полученные данные пришли от указанной ККС и не были модифицированы. При этом аутентификация КИ должна также предполагать проверку порядка следования и своевременность доставки сообщений.

Техника аутентификации данных в ККС предполагает присоединение к КИ созданного с использованием секретного ключа небольшого блока данных фиксированного размера, называемого криптографической контрольной суммой или кодом аутентификации сообщения (Message Authentication Code, MAC). При этом предполагается, что две участвующие в обмене данными стороны, ККС и потребитель, используют общий секретный ключ K . Чтобы послать сообщение M (КИ) потребителю B , отправитель (ККС) вычисляет код аутентификации сообщения как функцию сообщения и ключа:

$$MAC = C_K(M),$$

где M — сообщение переменной длины; K — секретный ключ, известный только отправителю (ККС) и получателю (потребителю); $C_K(M)$ — аутентификатор фиксированной длины.

Сообщение с добавленным к нему значением MAC пересылается потребителю КИ. Потребитель КИ выполняет аналогичные вычисления с полученным сообщением (КИ), используя тот же секретный ключ, чтобы вычислить новое значение MAC. Вычисленное значение MAC сравнивается с полученным вместе с сообщением (КИ) значением.

Для КИ, передаваемой национальной СДК, предлагается применять функцию вычисления значения MAC, называемую алгоритмом аутентификации данных (Data Authentication Algorithm), который основан на использовании DES [9].

ВЫВОДЫ

1. Киберугрозы представляют собой основной вызов для будущего применения ГНСС. Кибератаки могут воздействовать как на бортовые, так и на наземные системы, а методы воздействия могут простирались от простых асимметричных атак, типа глушения, до высокосложных электронных систем и программных атак.

2. С целью устранения атаки модификации на сервер ККС информация (внутренняя информация) о высоте фазового центра антенны НАП и параметрах опорного генератора обязательно должна шифроваться.

3. В качестве примера с помощью имитационного комплекса было проведено моделирование работы ККС в реальном времени. Показано, что применение MAC кода делает не возможной атаку на основе применения концепции VRS.

4. Самая простая кибератака на СДК основана на невозможности реализации надежного определения подлинности КИ в условиях применения «одностороннего» канала связи. Так как в этой ситуации хорошо срабатывает известная хакерская атака повторением сигнала (replay attack). Поэтому для контроля достоверности КИ обязательно требуется дублирующий радиоканал передачи данных, который достаточно сложно подавить средствами радиоэлектронной борьбы.

Литература

- [1] Українська мережа станцій космічної геодезії та геодинаміки (Укргеокоосмережа) / [О.В. Болотіна, С.Л. Болотін, М.М. Медведський та ін.] ; за ред. Я. С. Яцківа. — К.: ВАІТЕ, 2005. — 62 с.
- [2] Одуан К. Измерение времени. Основы GPS / Одуан К., Гино Б. ; пер. с англ. — Москва: Техносфера, 2002. — 400 с.

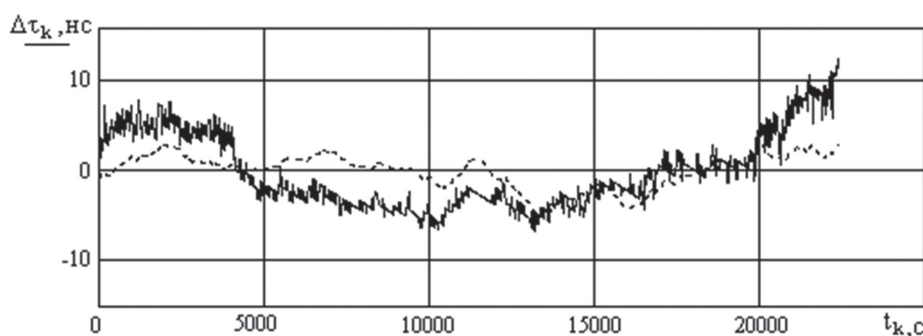


Рис. 8. Результат сглаживания с помощью цифрового рекурсивного фильтра

- [3] ГЛОНАСС. Принципы построения и функционирования / [Бакитко Р.В., Болденков Е.Н., Булавский Н.Т. и др.]; под ред. А.И. Перова, В.Н. Харисова. Изд. 4-е, перераб. и доп. — М: Радиотехника, 2010. — 800 с.
- [4] Глобальные навигационные спутниковые системы. Системы дифференциальной коррекции. Общие технические требования : ГОСТ Р 54459—2011 — [Дата введения — 2012—07—01]. — М. : Стандартинформ, 2012. — 18 с. (Национальный стандарт Российской Федерации).
- [5] Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, David Brumley. GPS Software Attacks. Proceedings of the ACM Conference on Computer and Communications Security (CCS), October 16–18, 2012, Raleigh, North Carolina, USA. (Nov28_GPS.pdf)
- [6] Nils Ole Tippenhauer, Christina Pupper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. Proceedings of the ACM Conference on Computer and Communications Security (CCS), 22:75–85, 2011.
- [7] Mark L. Psiaki, Brady W. O'Hanlon, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals. In Proceedings of the Institute of Navigation GNSS (ION GNSS 2011), September 2011.
- [8] Глобальная навигационная спутниковая система. Форматы передачи корректирующей информации. Технические требования : ГОСТ Р 53610-2009 — [Дата введения — 2011—01—01]. — М. : Стандартинформ, 2011. — 20 с. (Национальный стандарт Российской Федерации).
- [9] Горбенко Ю.И., Горбенко И.Д. Инфраструктуры открытых ключей. Электронный цифровой подпис. Теория та практика : монографія. — Харків: Видавництво «Форт», 2010. — 608 с.
- [10] Radio Technical Commission for Maritime Services Recommended Standards for Differential GNSS Service (RTCM SC-104) Version 2.2, 1998.
- [11] Система спутниковая навигационная глобальная. Термины и определения : ГОСТ Р 52928-2008 — [Дата введения — 2008—07—20]. — М. : Стандартинформ, 2008. — 11 с. (Национальный стандарт Российской Федерации).
- [12] Глобальная навигационная спутниковая система. Станция контрольно-корректирующая локальная гражданского назначения. Технические требования : ГОСТ Р 52866—2007 — [Дата введения — 2008—07—01]. — М. : Стандартинформ, 2008. — 7 с. (Национальный стандарт Российской Федерации).
- [13] National Marine Electronics Association (NMEA 0183) Standard for Interfacing Marine Electronic Devices (Version 2.30), 1998.
- [14] Interface Control Document: NAVSTAR GPS Space Segment/ Navigation User Interfaces (ICD-GPS-200). — Rockwell Int. Corp., 1997.
- [15] Устройство временной синхронизации с использованием сигналов GPS/ГЛОНАСС “NAVIOR-S” CH-3834. Руководство эксплуатации ТДЦК.461513.030 РЭ. — 2000. — 38 с.
- [16] Аппаратура потребителей спутниковых навигационных систем ГЛОНАСС и NAVSTAR. Протокол обмена BINR. ПКАН.461513.015 Д2. — 2000. — 35 с.

- [17] Чирков А.Г., Матисов Б.Г. Современная теория стабильности прецизионных генераторов. СПб. Издательство Политехнического университета, 2005. — 355 с.

Поступила в редколлегию 29.04.2013



Гриненко Татьяна Алексеевна, канд. тех. наук, ст. преподаватель кафедры БИТ ХНУРЭ. Научные интересы: методы и средства криптографической защиты информации.



Нарежний Алексей Павлович, старший научный сотрудник отдела, Метрологический центр военных эталонов Вооруженных Сил Украины. Научные интересы: частотно-временные измерения и системы единого времени.

УДК 621.317.76.089.68:621.373.82

Застосування кодів автентифікації повідомлень для виявлення модифікацій даних у регіональних системах диференціальної корекції навігаційних сигналів систем GPS/ГЛОНАСС / Т.О. Гріненко, О.П. Нарежний // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 301–310.

У статті обґрунтовується необхідність застосування кодів автентифікації повідомлень (MAC) для забезпечення цілісності і достовірності коригуючої інформації, що формується системами диференціальної корекції навігаційних сигналів систем GPS/ГЛОНАСС. На прикладі роботи типової схеми контрольно-коригуючої станції обґрунтовується необхідність застосування MAC-алгоритмів при передачі “сирих” вимірів уточнених ефемерид і частотно-часових поправок навігаційно-космічних апаратів глобальних навігаційних супутникових систем GPS/ГЛОНАСС.

Ключові слова: контрольно-коригуюча станція, захист даних, криптографія, коди автентифікації повідомлень.

Лл.: 08. Бібліогр.: 17 найм.

UDC 621.317.76.089.68:621.373.82

Message authentication codes application for data modification detection in regional systems of differential correction of GPS/GLONASS systems navigation signals / T.O. Grinenko, O.P. Nareznyi // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 301–310.

The paper substantiates the need of message application codes (MAC) application for ensuring integrity and validity of correction information formed by differential correction systems of GPS/GLONASS systems navigation signals. The need of MAC-algorithms application during transmission of raw measurement data of specified ephemeris and frequency and time corrections of space navigation vehicles of GPS/GLONASS global navigation satellite systems is substantiated using an example of the operation of a control-correction station typical scheme.

Keywords: control correction station, data protection, cryptography, message authentication codes.

Fig.: 08. Ref.: 17 items.

МЕТОДЫ И МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 629.735

КЛАССИФИКАЦИЯ МЕТОДОВ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ К БЕЗОПАСНОСТИ ПРОДУКТОВ И СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

А.В. ПОТИЙ, Д.С. КОМИН, Ю.Н. КОЗЛОВ

Рассмотрены вопросы использования терминов «доверие» и «гарантии» в области оценки безопасности ИТ, как аутентичные английскому термину *assurance*, даны их определения, контекст и область использования. Приводится классификация методов обеспечения доверия к безопасности продуктов и систем ИТ.

Ключевые слова: доверие, гарантии безопасности, единые критерии.

ВВЕДЕНИЕ

Неотъемлемой частью современных систем и продуктов информационных технологий (ИТ) является комплекс мер по обеспечению безопасности информации, которая хранится, циркулирует или обрабатывается в этих системах (продуктах), особенно — если это информация с ограниченным доступом. Очевидно, что безошибочное, устойчивое и безопасное функционирование систем ИТ практически невозможно осуществить в течение всех стадий ее жизненного цикла вследствие сбоев, ошибок оператора, отказов оборудования, неудовлетворительной организации процесса разработки, недооценки угроз и т.д. Из этого следует, что ошибки, уязвимости и риски будут существовать всегда и изменяться на всех стадиях жизненного цикла системы ИТ. Следовательно, ошибками, уязвимостями и рисками надо управлять в пределах допустимых параметров, т.е., используя технические и организационные меры, необходимо обеспечить приемлемый (в конкретных условиях эксплуатации) уровень доверия (*assurance*) к системе ИТ. Приемлемое доверие означает удовлетворение системы ИТ специальным заранее определенным требованиям, которые определяются исходя из целей и требований безопасности. Доверие не обеспечивает предоставление объекту каких-либо дополнительных мер безопасности или услуг, а способствует снижению рисков, поскольку уменьшает неопределенность, связанную с уязвимостями системы/объекта ИТ. Существуют различные методы обеспечения доверия, использование которых зависит от объекта оценки, целей и политики безопасности и ряда других факторов. В данной статье на основе анализа существующих методов доверия проведена их классификация. Также рассмотрены вопросы терминологии в отношении термина *assurance*, поскольку в зависимости от контекста использования оно может иметь различный перевод (доверие, гарантии) и различное значение.

1. ASSURANCE – ДОВЕРИЕ ИЛИ ГАРАНТИИ?

Термин *assurance* в среде безопасности информационных технологий используется для описания мер по оценке уязвимостей и остаточных рисков оцениваемого объекта. Забегая вперед, можно сказать, что *assurance* — это современный подход по оценке доверия к безопасности продуктов и систем информационных технологий.

В среде специалистов по информационной безопасности существуют разногласия относительно перевода данного термина на украинский и русский языки. Одни специалисты при переводе с английского используют термин *гарантии*, в то время как другие — термин *доверие*. Ранее этот вопрос исследовался в работах [1, 2], однако при переводе данного термина необходимо учитывать контекст его использования.

Современное понимание подходов оценки информационной безопасности тесно связано с использованием неформальных методов оценивания, и, как следствие, с получением качественных результатов их применения. Вследствие этого значительное место в принятии решений по оценке и понимании результатов такого оценивания потребителем имеют субъективные и психологические факторы. В [1] исследовалось толкование термина *доверие* различными словарями. Например, доверие — уверенность в чьей-нибудь добросовестности, искренности, в правдивости чего-нибудь; психическое состояние, в силу которого мы полагаемся на какое-либо мнение, кажущееся нам авторитетным, и потому отказываемся от самостоятельного исследования вопроса, могущего быть нами исследованным и др. Поэтому перевод термина *assurance* как доверие является оправданным при характеристике общей системы безопасности ИТ в целом, независимо от объекта оценивания (продукт или система ИТ, услуга обеспечения безопасности, процесс, персонал, организация и др.).

Из [3, 4] следует понимать, что доверие является такой характеристикой, которая способствует снижению риска, поскольку уменьшает неопределенность, связанную с уязвимостями объекта, таким образом, уменьшая его потенциальную уязвимость и приводя к снижению общего риска, связанного с объектом.

Таким образом, *доверие* — состояние субъекта, вовлеченного в систему создания и использования продуктов и систем ИТ (разработчик, продавец, оценщик, потребитель), характеризующее меру его уверенности в том, что оцениваемый объект соответствует своим целям безопасности. А понятие *обеспечения доверия* следует понимать как совокупность процессов (мероприятий, действий, процедур), направленных на формирование у заинтересованных субъектов доверия к безопасности продуктов и систем ИТ.

С другой стороны термин *assurance* используется в международном стандарте ISO/IEC 15408 [5, 6] (Критерии оценки безопасности информационных технологий) в качестве *системы требований*, которые характеризуют степень корректности реализации функциональных услуг безопасности оцениваемого объекта. В национальном стандарте НД ТЗИ 2.5-004-99 [7] такие требования именуется *требованиями гарантий*, в то время как в ГОСТ Р ИСО/МЭК 15408 [8] (национальный стандарт Российской Федерации) *требованиями доверия*. В [2] проанализированы толкования слов доверие и гарантии на предмет возможности их использования в контексте критериев оценки безопасности ИТ. Сделан вывод, что термин *гарантии*, в данном контексте, является более подходящим по смыслу, значению и адекватности английскому термину *assurance*.

Таким образом, в терминологии информационной безопасности можно выделить два толкования английского термина *assurance*. С одной стороны это *гарантии* — набор требований, характеризующий средства, способы и условия обязательные (или рекомендованные) к выполнению в течение всего жизненного цикла ИТ-продукта для обеспечения корректной реализации функциональных услуг безопасности, противостояния угрозам безопасности и обеспечения требуемого уровня защищенности ИТ-продукта [1]; а, с другой стороны, *доверие* — мера уверенности в том, что оцениваемый объект соответствует своим целям безопасности, и связанное с ним понятие *обеспечения доверия* — совокупность процессов, направленных на формирование у заинтересованных субъектов доверия к безопасности продуктов и систем ИТ [3, 4]. При этом *оценка объекта на соответствие требованиям гарантий* является одним из методов обеспечения доверия к безопасности продуктов и систем ИТ.

2. КЛАССИФИКАЦИЯ МЕТОДОВ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ

Существует большое количество методов обеспечения доверия. Выбор необходимого ме-

тода обеспечения доверия должен основываться на изучении политики безопасности организации, бизнес требований и вида оцениваемого объекта. Также, немаловажным фактором выбора метода обеспечения доверия является наличие имеющихся ресурсов (временных, кадровых, финансовых и др.). Поэтому для выбора и применения какого-либо метода обеспечения доверия правообладателям могут потребоваться рекомендации специалистов.

Анализ методов доверия позволил их классифицировать:

1) по объекту оценивания:

- оценивание продукта (системы) ИТ;
- оценивание процессов (разработки, создания, функционирования);
- оценивание внешних факторов (среда, организация, персонал и др.);
- комбинированные (уровень 1 ... уровень 7);

2) по региону использования:

- региональные (национальные);
- международные;

3) по юридической силе:

- национальные;
- «де-факто»;

4) по уровню строгости:

- формальные;
- неформальные;

5) по охвату стадий жизненного цикла:

- проектирование/разработка;
- интеграция;
- ввод в эксплуатацию;
- эксплуатация;
- комбинированные;

6) по типу доверия:

- доверие к корректности;
- доверие к эффективности.

Высокоуровневая классификация методов обеспечения доверия выделяет основные три направления: оценивание продукта, оценивание процесса и оценивания внешних факторов. При оценке продукта проверяется непосредственно сам объект и связанная с ним проектная документация по безопасности, независимо от процессов разработки. Наиболее значимыми стандартами, регламентирующими метод обеспечения доверия к продуктам, является международный стандарт ISO/IEC 15408 [5] и национальный стандарт НД ТЗИ 2.5-004-99 [7], и связанные с ними работы, в которых представлен метод оценки гарантий информационной безопасности [1, 9, 10]. Оценка процессов включает в себя проверку организационных процессов используемых для производства и эксплуатации объекта в течение его жизненного цикла. Основные из многочисленных методов обеспечения доверия к процессам закреплены в стандартах ISO/IEC 21827 (проектирование безопасности работы систем — модель зрелости) и ISO/IEC 15504 (оценка программного процесса) [11–13]. Оценка внешних факторов включает в себя проверку влияния

условий окружающей среды, вносящих вклад в качество процессов производства и функционирования. К таким факторам относятся персонал и физическая среда. К методам обеспечения доверия к внешним факторам можно отнести ISO 9000 (менеджмент качества). Также актуальным и перспективным направлением в развитие методов обеспечения доверия к внешним факторам, и в частности к персоналу, является разработка методов обеспечения и оценки культуры информационной безопасности [14, 15]. Существуют также комбинированные методы обеспечения доверия, которые охватывают как все объекты оценивания (оценивание продукта, оценивание процесса и оценивания внешних факторов), так и их часть. Классификация методов обеспечения доверия по уровню охвата объектов оценивания представлена в табл. 1:

Таблица 1

Уровни охвата объектов оценки методами обеспечения доверия

Уровень	Доверие к продукту	Доверие к процессу	Доверие к внешним факторам
1	+		
2		+	
3			+
4	+	+	
5	+		+
6		+	+
7	+	+	+

Методы обеспечения доверия к безопасности могут быть закреплены как в национальных (действующих на территории одного государства или региона), так и международных стандартах (как правило, изданных под эгидой Международной организации по стандартизации (ISO)). Примерами национальных стандартов являются нормативные документы НД ТЗІ 2.5-004-99 и НД ТЗІ 2.7-010-09, которые имеют юридическую силу только на территории Украины. К международным стандартам можно отнести ISO/IEC 15408, ISO/IEC 15288 (процессы жизненного цикла системы), ISO/IEC 13335 (руководство по управлению безопасностью ИТ) и др.

Методы обеспечения доверия включают в себя как официальные национальные и международные стандарты, так и стандарты «де-факто» и другие общепринятые методы. Примером стандарта «де-факто» является метод оценки SSE-CMM (SSAM), который является детально документированным методом доверия, однако не является ни национальным, ни международным стандартом. Другим примером стандарта «де-факто» является метод ТРЕР (надежный процесс оценивания продукта), который, несмотря на распространенность и успешное использование в некоторых государственных учреждениях, также не является стандартом.

По уровню строгости научные методы принято классифицировать как формальные, полужформальные и неформальные. К неформальным методам относятся те, выводы и заключения по которым производятся на основании данных (значений), выраженных словами, словосочетаниями или предложениями (лингвистическими терминами) и которые не могут получить количественной оценки. Получение количественных оценок при оценке доверия к безопасности является сложной задачей, ввиду чего подавляющее большинство стандартов, описывающих методы обеспечения доверия, можно отнести к неформальным. Для формализации неформальных методов можно использовать подход, который лежит в основе метода оценки гарантий информационной безопасности [1, 9, 10] и использует математический аппарат лингвистических переменных и нечеткого логического вывода. Другая классификация строгости доверия предложена в ГОСТ Р 54583-2011 [3, 4], суть которой отображена в табл. 2:

Таблица 2

Строгость доверия и его использование

Уровень строгости	Использование доверия
1	Простая «печать утверждения доверия»
2	Заявления о доверии позитивного уровня
3	Конкретные факты, поддерживающие заявленное доверие
4	Конкретные факты, поддерживающие заявленное доверие, которое можно верифицировать
5	Предоставление доверия общей аудитории, например, совету директоров, и признание этой аудиторией
6	Представление доверия аудитории из специалистов по безопасности и признание этой аудиторией

По охвату стадий жизненного цикла методы обеспечения доверия могут предназначаться как для конкретной стадии, так и для нескольких стадий жизненного цикла (рис. 1). Например, метод обеспечения доверия, предоставляемый стандартом ISO/IEC 15408, охватывает все стадии жизненного цикла оцениваемого объекта (проектирование, разработка, интеграция, ввод в эксплуатацию, эксплуатация); метод SE-CMM (модель технологической зрелости системного проектирования) — охватывает только две стадии: стадию проектирования и стадию интеграции; метод ISO/IEC 17799 (практические правила управления информационной безопасностью) — охватывает только стадию функционирования.

Среди методов обеспечения доверия также различают методы обеспечения доверия к эффективности и доверия к корректности. При обеспечении доверия к корректности дается ссылка на оценку объекта с целью верификации корректности его внедрения в соответствии с

проектом. Напротив, доверие к эффективности относится к способности функций безопасности объекта противостоять осознанным или идентифицированным угрозам. С целью получения общего доверия объект должен быть оценен как на предмет корректности проекта, внедрения и эксплуатации (элемент корректности), так и должен обладать соответствующими функциональными возможностями обеспечения безопасности для противостояния идентифицированным угрозам (элемент эффективности).

ЗАКЛЮЧЕНИЕ

Одно из ключевых мест в области оценки безопасности продуктов и систем ИТ принадлежит английскому термину *assurance*. В зависимости от контекста использования может переводиться как *гарантии*, либо *доверие*. Доверие характеризует меру уверенности субъекта в том, что система ИТ соответствует своим целям безопасности, а методы обеспечения доверия являются совокупностью процессов, направленных на формирование у субъектов доверия к безопасности ИТ. Гарантии же являются системой требований, оценка которых позволяет судить о корректности реализации функций безопасности в системе ИТ. Таким образом, оценка объекта на соответствие требованиям гарантий является одним из методов обеспечения доверия к безопасности продуктов и систем ИТ.

Анализ методов обеспечения доверия позволил провести их классификацию. В статье методы обеспечения доверия классифицированы: по объекту оценивания; по региону использования; по уровню строгости; по охвату стадий жизненного цикла; по типу доверия. Классификация позволяет облегчить поиск и выбор необходи-

мого метода доверия в зависимости от условий эксплуатации и целей безопасности системы или продукта ИТ.

Литература

- [1] Потий А.В. Системно-онтологический анализ предметной области оценивания гарантий информационной безопасности / А.В. Потий, Д.С. Комин // Радиоелектронні і комп'ютерні системи. Науково-технічний журнал. – 2010. – № 5(46). – С. 50–56.
- [2] Потий А.В. Оценка гарантий информационной безопасности на основе функционально-лингвистического подхода / А.В. Потий, Д.С. Комин // Прикладная радиоэлектроника. – 2010. – Том 9. – № 3. – С. 421–435.
- [3] ISO/IEC TR 15443-1:2005, Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework.
- [4] ГОСТ Р 54581-2011/ISO/IEC TR 15443-1:2005, Информационная технология – Методы и средства обеспечения безопасности – Основы доверия к безопасности – Часть 1: Обзор и основы.
- [5] ISO/IEC 15408-1:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
- [6] ISO/IEC 15408-3:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirement.
- [7] НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.
- [8] ГОСТ Р ИСО/МЭК 15408-1, Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель.

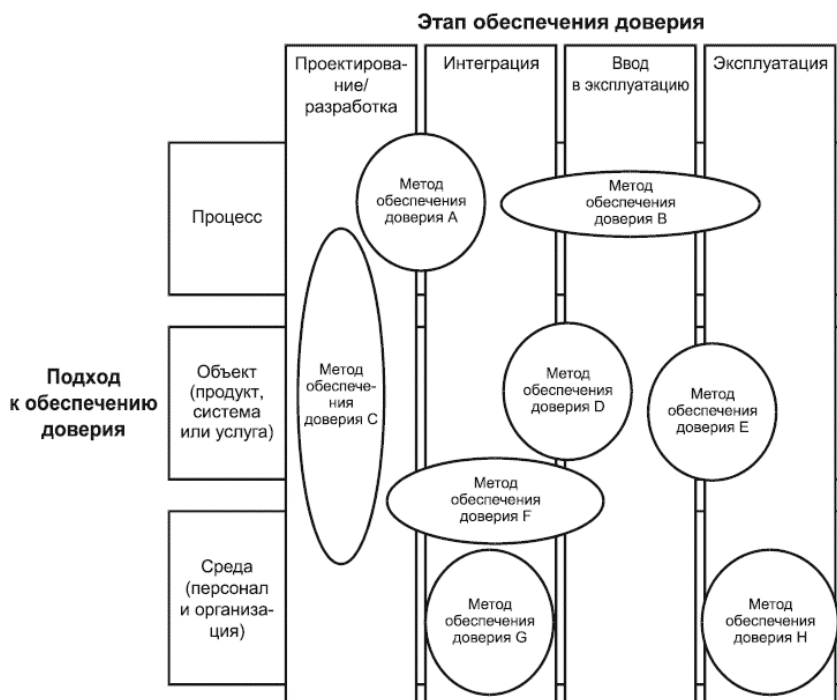


Рис. 1. Охват стадий жизненного цикла методами обеспечения доверия

- [9] *Потий А.В.* Формальное описание процесса оценивания гарантий информационной безопасности / А.В. Потий, Д.С. Комин, В.И. Новиков // Системы управления, навигации та зв'язку. — 2011. — № 4 (20). — С. 246–249.
- [10] *Потий А.В.* Метод оценивания требований гарантий информационной безопасности / А.В. Потий, Д.С. Комин // VI-я Международная научно-практическая конференция «Наука и социальные проблемы общества: информатизация и информационные технологии». Сборник научных трудов. — Харьков: ХНУРЭ, 2011. — С. 221–222.
- [11] *Потий О.В.* Формалізована модель діяльності із захисту інформації / О. В. Потій // Радіоелектронні і комп'ютерні системи. — 2007. — №6 (25). — С. 96–103.
- [12] *Потій О.В.* Методичні аспекти оцінки зрілості процесів захисту інформації в умовах невизначеності / О. В. Потій, А.В. Леншин // Прикладна радіоелектроніка. — 2006. — Том 5, №1. — С. 134–138.
- [13] *Потій О.В.* Онтологічні моделі властивостей зрілості процесів захисту інформації / О. В. Потій, // Прикладна радіоелектроніка. — 2009. — Том 8. — С. 112–120.
- [14] *Потій О.В.* Властивості діяльності із забезпечення захисту інформації як системної категорії / О.В. Потій, Д.Ю. Пилипенко // Прикладна радіоелектроніка. — 2012. — Том 11. — № 2. — С. 299–303.
- [15] *Potiy A.V.* The prerequisites of information security culture development and an approach to complex evaluation of its level / A.V. Potiy, D.Y. Pilipenko, I.N. Rebriy // Радіоелектронні і комп'ютерні системи. — № 5 (57). — 2012. — С. 72–77.

Поступила в редколлегию 12.05.2014

Потий Александр Владимирович,
фото и сведения об авторе см. на стр. 260.



Комин Дмитрий Сергеевич, кандидат технических наук, научный сотрудник научного центра Воздушных Сил Харьковского университета Воздушных Сил им. И. Кожедуба. Научные интересы: методы системного анализа процессов защиты информации; методы оценки безопасности объектов информационной деятельности.

Козлов Юрий Николаевич, фото и сведения об авторе см. на стр. 260.

УДК 629.735

Класифікація методів забезпечення довіри щодо безпеки продуктів та систем інформаційних технологій / О.В. Потій, Д.С. Комін, Ю.М. Козлов // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 311–315.

Розглянуто питання використання термінів «довіра» та «гарантії» в області оцінки безпеки ІТ, як аутентичні англійському терміну assurance, надано їх визначення, контекст та область використання. Наводиться класифікація методів забезпечення довіри щодо безпеки продуктів та систем ІТ.

Ключові слова: довіра, гарантії безпеки, єдині критерії оцінки інформаційної безпеки.

Табл.: 2. Іл.: 1. Бібліогр.: 15 найм.

UDK 629.735

Classification of methods of trust assurances to security of IT products and systems / A.V. Potiy, D.S. Komin, Yu.N. Kozlov // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 311–315.

Translation problems of the term «assurances» in the IT security sphere are considered. A classification of security assurances methods to IT systems and products is presented.

Keywords: trust, security assurances, common criteria.

Tab.: 1. Fig.: 1. Ref.: 15 items.

БЫСТРОДЕЙСТВУЮЩИЙ ДЕТЕРМИНИРОВАННЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ПОТОКОВОГО ШИФРОВАНИЯ

А.А. ТОРБА, В.А. БОБУХ, А.А. БОБКОВА

В работе проанализированы некоторые недостатки известного аппаратного алгоритма потокового шифрования А5 и предложен аппаратный быстродействующий генератор псевдослучайных последовательностей, в значительной мере устраняющий недостатки известного алгоритма.

Ключевые слова: алгоритм А5, генератор псевдослучайных последовательностей.

ВВЕДЕНИЕ

Максимальная скорость передачи информации в каналах связи с ограниченным доступом определяется быстродействием аппаратных (или программно-аппаратных) алгоритмов шифрования и расшифрования сообщений.

Наибольшим быстродействием среди известных симметричных алгоритмов криптографических преобразований обладают потоковые алгоритмы, которые позволяют формировать каждый очередной бит псевдослучайной гаммы за один такт синхронизации.

Согласно Райнеру Рюппелю можно выделить четыре основных подхода к проектированию поточных шифров:

- Системно-теоретический подход основан на создании для криптоаналитика сложной, ранее неисследованной проблемы.
 - Сложностно-теоретический подход основан на сложной, но известной проблеме (например, факторизация чисел или дискретное логарифмирование).
 - Информационно-технический подход основан на попытке утаить открытый текст от криптоаналитика — вне зависимости от того сколько времени потрачено на дешифрование, криптоаналитик не найдёт однозначного решения.
 - Рандомизированный подход основан на создании объёмной задачи; криптограф тем самым пытается сделать решение задачи расшифрования физически невозможной.
- Теоретические критерии Райнера Рюппеля для проектирования поточных систем:
- длинные периоды выходных последовательностей;
 - большая линейная сложность;
 - диффузия — рассеивание избыточности в подструктурах, «размазывание» статистики по всему тексту;
 - каждый бит потока ключей должен быть сложным преобразованием большинства битов ключа;
 - критерий нелинейности для логических функций.

1. АЛГОРИТМ ПОТОКОВОГО ШИФРОВАНИЯ А5

Известный потоковый алгоритм шифрования А5 используется для обеспечения конфиденциальности передаваемых данных между телефоном и

базовой станцией в европейской системе мобильной цифровой связи GSM (Group Special Mobile).

Шифр основан на побитовом сложении по модулю два (булева операция XOR) генерируемой псевдослучайной последовательности и шифруемой информации [1].

В А5 псевдослучайная последовательность гаммы реализуется на основе трёх линейных рекуррентных регистров (ЛРР) сдвига с обратной связью. Регистры имеют длины: $L(R1) = 19$, $L(R2) = 22$ и $L(R3) = 23$ бита (рис. 1). Сдвигами управляет специальная схема. В каждом регистре есть биты синхронизации: $R1(8)$, $R2(10)$ и $R3(10)$, над которыми вычисляется мажоритарная функция:

$$F = (x \& y) \vee (x \& z) \vee (y \& z),$$

где x, y, z — биты синхронизации.

В каждом такте сдвигается только тот регистр, у которого бит синхронизации равен функции F , т.е. на каждом шаге смещается два или три регистра, что приводит к их неравномерному движению. Результирующая псевдослучайная последовательность формируется путём операции XOR над выходными битами трех регистров (рис. 1).

Недостатком алгоритма А5 является недопустимо малая криптостойкость, которая определяется длиной сеансового ключа — 64 бита (определяемой суммарной длиной всех ЛРР), поэтому сложность атаки, основанной на прямом переборе, не превышает 2^{64} .

Учитывая, что в алгоритме А5 принудительно обнулены 10 бит ключа [1], — криптостойкость этого алгоритма даже ниже, чем у алгоритма DES (с длиной ключа — 56 бит).

Практика показывает, что свыше 40 % сеансовых ключей в алгоритме А5 приводят к минимальной длине периода генерируемой псевдослучайной последовательности, а именно: $T = 2^{23} - 1$.

Известна также атака Андерсона на открытом тексте, основанная на предположении о содержании первых двух ЛРР и попытке определения самого длинного третьего ЛРР по ключевой последовательности.

2. АЛГОРИТМ ПОТОКОВОГО ШИФРОВАНИЯ AUGUST-1

Детерминированный генератор псевдослучайных последовательностей для потокового

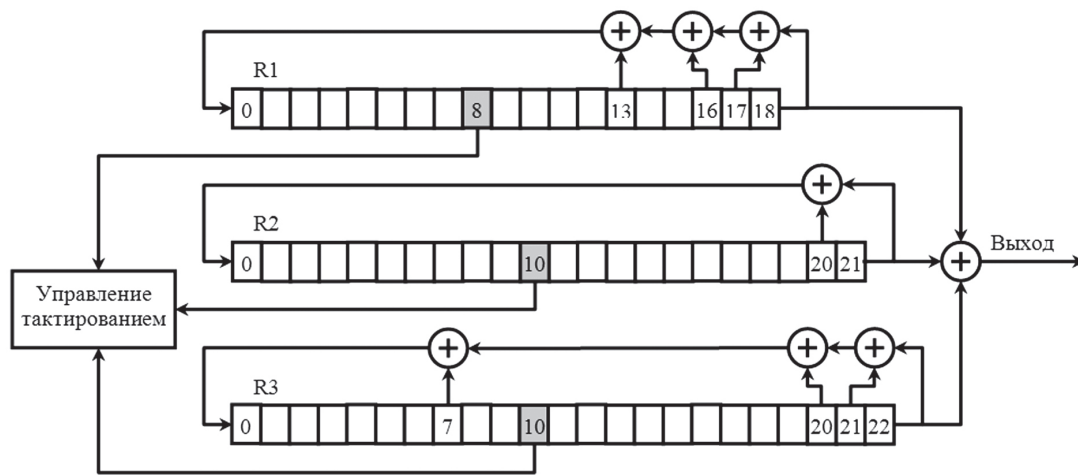


Рис. 1

шифрования AUGUST-1, описанный в патенте Украины [2], позволяет в значительной мере устранить указанные недостатки алгоритма А5. Упрощенная структурная схема этого генератора приведена на рис. 2.

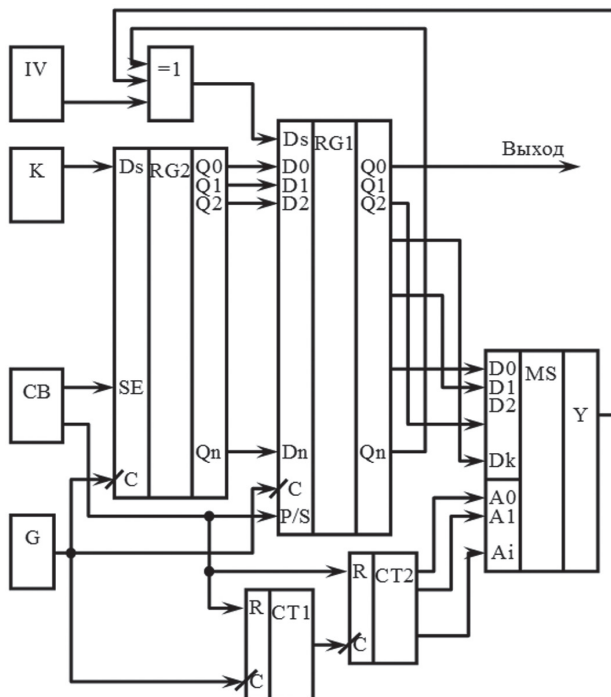


Рис. 2

Основу генератора составляет линейный рекуррентный регистр (ЛРР), реализованный на сдвигающем регистре (RG1). На информационный вход последовательного сдвига (Ds) этого регистра подается сигнал с выхода элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» (элемента «XOR»), а к входам этого элемента подключены: последний выход сдвигающего регистра «Qn» и выход мультиплексора MS.

На информационные входы (D1...Dk) мультиплексора (MS) подаются сигналы с отводов сдвигающего регистра (RG1). Номера всех отводов m_k должны удовлетворять известному условию для ЛРР: полином, вычисленный на коэффициентах $-1 + x^m + x^n$ — должен быть примитивным и неприводимым над полем Галуа.

На адресные входы мультиплексора MS ($A0...Ai$) подаются выходные сигналы двоичного счетчика СТ2. Коэффициент деления счетчика СТ1 определяет периодичность смены параметров рекурренты (обычно эта периодичность во много раз меньше разрядности сдвигающего регистра «n»). Желательно выбирать коэффициент деления счетчика СТ1 и длину ЛРР (т.е. разрядность «n» сдвигающего регистра RG1) как взаимно простые числа.

Известные математические алгоритмы, которые позволяют вычислить параметры рекурренты псевдослучайных генераторов на основе ЛРР (т.е. рассчитать основные параметры — «m» и «n») по результатам наблюдения выходной битовой последовательности, длительность которой в несколько раз превышает разрядность сдвигающего регистра, — в данном случае являются бесполезными, — потому что параметр «m» за время наблюдения многократно изменится.

Скорость формирования псевдослучайной последовательности определяется частотой тактового генератора (G) и может составлять от 10 МГц до 1 ГГц.

До начала шифрования абоненты обмениваются секретными кратковременными (или сеансовыми) ключами Кс. Алгоритм Диффи-Хеллмана (англ. Diffie-Hellman, D-H) позволяет двум или более пользователям обменяться без посредников секретным ключом, который будет использован затем для симметричного шифрования.

Длина секретного ключа Кс в битах определяет криптостойкость алгоритма потокового шифрования и равняется разрядности «n» сдвигающего регистра RG1. При использовании современных программируемых логических интегральных схем (ПЛИС) разрядность регистра RG1 (и секретного ключа Кс) может составлять от 100 до нескольких тысяч бит.

До начала шифрования сформированный секретный ключ Кс вводится в параллельный регистр RG2. Для этого блок управления (CB) вырабатывает сигнал разрешения последовательного ввода (SE), который поступает на вход управления параллельного регистра RG2.

После ввода секретного ключа в регистр RG2 — этот ключ в параллельном формате записывается в регистр сдвига RG1. Для этого блок управления (СВ) формирует логический сигнал, который переводит первый регистр RG1 в режим параллельной загрузки, а также удерживает в нулевом состоянии первый и второй счетчики СТ1, СТ2.

Перед шифрованием в канал связи передается случайное значение инициализации IV (Initialisation Value или синхропосылка). Это значение инициализации не является секретным и передается по открытому каналу связи перед каждым сеансом шифрования. Использование для всех сообщений отдельных случайных значений инициализации IV позволяет формировать различные значения псевдослучайной гаммы для каждого нового сообщения. При этом даже одинаковые начальные тексты сообщений будут зашифрованы по-разному.

Одновременно с передачей в канал связи значение инициализации IV в последовательном формате вводится в сдвигающий регистр RG1 через третий вход элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» (элемента «XOR»). На первый и второй входы этого элемента «XOR» подаются сигналы с последнего выхода последовательного регистра RG1 и выхода мультиплексора MS для формирования рекуррентной псевдослучайной последовательности гаммы.

Для смены параметров рекурренты первого регистра сдвига RG1 его логические уровни с промежуточных выходов m_k подаются на информационные входы мультиплексора MS, а адресные входы этого мультиплексора подключены к выходам второго счетчика СТ2.

Выходная псевдослучайная последовательность гаммы, которая может сниматься с любого выхода первого регистра сдвига RG1, является детерминированной (т.е. может быть полностью восстановлена на приемной стороне канала связи) и зависит от секретного значения кратковременного сеансового ключа Кс, от случайного значения инициализации IV и долговременных секретных параметров (ключей): длины секретного ключа « n », таблицы коммутации мультиплексора MS и коэффициента деления первого счетчика СТ1.

Секретное значение длины « n » кратковременного сеансового ключа Кс делает бессмысленной лобовую атаку по перебору всех значений ключа.

ВЫВОДЫ

Предложенный и запатентованный быстродействующий детерминированный генератор псевдослучайных последовательностей для потокового шифрования AUGUST-1 позволяет устранить большинство недостатков известного алгоритма А5. Криптостойкость предложенной системы потокового шифрования определяется разрядностью кратковременного секретного ключа Кс, которая может составлять от 100 до не-

скольких тысяч бит. Причем секретным является не только значение ключа Кс, но и его длина.

Скорость формирования псевдослучайной последовательности ограничивается быстродействием используемых логических микросхем и может достигать 1000 МГц.

Литература

[1] <http://ru.wikipedia.org/wiki/A5>.

[2] Патент Украины на полезную модель № 85039, опубл. Бюл. № 21, 2013 г.

Поступила в редколлегию 28.05.2014



Торба Александр Алексеевич, кандидат технических наук, доцент кафедры ЭВМ ХНУРЭ. Научные интересы: аппаратные средства криптографических систем.



Бобух Всеволод Анатольевич, кандидат технических наук, начальник отдела аппаратных средств АО «ИИТ». Научные интересы: аппаратные средства криптографических систем.



Бобкова Анна Александровна, кандидат технических наук, доцент кафедры ПИ ХНУРЭ. Научные интересы: аппаратно-программные средства криптографических систем.

УДК 681.324.067

Швидкодійний детермінований генератор псевдовипадкових послідовностей для потокового шифрування / А.А. Торба, В.А. Бобух, А.А. Бобкова // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 316–318.

У роботі проаналізовано деякі недоліки відомого апаратного алгоритму потокового шифрування А5 та запропоновано апаратний швидкодійний генератор псевдовипадкових послідовностей, який значною мірою усуває недоліки відомого алгоритму.

Ключові слова: алгоритм А5, генератор псевдовипадкових послідовностей.

Л.: 2. Бібліогр.: 2 найм.

UDC 681.324.067

The high-speed determined generator of pseudo-random sequences for flow encryption / A.A. Torba, V.A. Bobukh, A.A. Bobkova // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 316–318.

Some imperfections of known hardware flow encryption algorithm A5 are analyzed and a hardware high-speed generator of pseudo-random sequences to a great extent eliminating imperfections of the known algorithm is offered in the paper.

Keywords: algorithm A5, generator of pseudo-random sequences.

Fig.: 2. Ref.: 2 items.

ДОСТАТОЧНЫЕ УСЛОВИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЭЛЕКТРОННЫХ СИСТЕМАХ

В.А. ГОРБАЧЕВ

Рассматриваются субъектно-объектная модель доступа, аксиоматические достаточные условия защищенности информации, а также требования, предъявляемые к мониторам безопасности в электронных системах.

Ключевые слова: политика безопасности, модель доступа, разграничения доступа, монитор безопасности, электронная система.

ВВЕДЕНИЕ

В настоящее время перед отечественными разработчиками сложных электронных систем (ЭС) стоят две противоречивые задачи:

1) реализовать довольно высокие требования безопасности к обработке информации;

2) сохранить в полном объеме совместимость с используемыми зарубежными электронными компонентами.

Основное противоречие состоит в том, что требование совместимости с зарубежными компонентами подразумевает их использование в составе защищенной системы. В то же время разработчики этих компонентов не ставили перед собой такой задачи в силу ориентации этих продуктов на массовый рынок. Поэтому встраивать дополнительные средства защиты в системы обработки информации специального назначения — занятие безнадежное, особенно в условиях отсутствия подробной технической документации и поддержки со стороны разработчиков этих компонентов. Таким образом, решение проблемы построения защищенных ЭС на базе таких компонентов является более чем актуальной задачей, причем ее решение требует развития новых подходов к проблеме проектирования защищенных ЭС.

Перед разработчиками современных электронных систем, предназначенных для обработки важной информации, стоят следующие задачи, требующие эффективного решения:

1) технологии проектирования должны основываться на принципах доказательно обеспечивающих гарантии защищенности систем;

2) интеграция средств защиты информации в процесс ее обработки в качестве обязательного элемента;

3) включение в механизмы защиты функций, обеспечивающих безопасность электронной системы в условиях возможного появления внутри ее компонентов, осуществляющих деструктивные действия.

Теоретические исследования, касающиеся моделей политики безопасности, ориентированы на программные системы [2, 3, 5] и не преследуют цель анализа безопасности информации в ЭС.

Целью данного исследования являются технологии проектирования защищенных ЭС, обеспечивающих устойчивость к деструктивному воздействию внутренних компонентов.

1. СУБЪЕКТНО-ОБЪЕКТНАЯ МОДЕЛЬ ЭС

Рассмотрим основные понятия субъектно-объектной модели ЭС. В ЭС действует дискретное время t . В каждый фиксированный момент времени t ЭС представляет собой конечное множество компонентов, разделяемых на два подмножества: субъектов доступа S ; объектов доступа O .

Определим эти абстрактные понятия и поставим им в соответствие физические представления в ЭС.

Объект (O_i) — часть ресурсов системы, находящаяся в момент времени t в пассивном состоянии относительно информации, а также других компонентов этой системы. Объект может быть источником нового субъекта, через процессы, которые локализованы в субъектах.

Субъект (S_j) — это компонент системы, находящийся в момент времени t в активном состоянии, который может изменять состояние системы с помощью субъектов. Субъекты могут порождать новые объекты и субъекты в системе.

Будем считать, что все компоненты ЭС в различные моменты времени t_k могут представлять собой либо субъекты, либо объекты. Кроме того, предполагается, что в любой момент времени t , в том числе и в начальный, множество субъектов доступа S не пусто.

Источник угроз электронной системы, в дальнейшем **источник угроз (ИУ)**. В пассивном состоянии это совокупность объектов, в активном состоянии это субъект и связанные с ним объекты.

Рассматривая ИУ, как некоторый тип субъекта, который способен осуществить несанкционированный доступ, отметим следующие его особенности.

Во-первых, ИУ, являясь аппаратным, программно-аппаратным ресурсом ЭС, в пассивном состоянии может быть частью некоторого объекта.

Во-вторых, угрозы информации в ЭС могут исходить только от активного субъекта — ИУ, ко-

торый в текущий момент времени владеет функцией управления ресурсами.

В-третьих, субъекты могут влиять друг на друга через изменяемые ими объекты. Одним из результатов воздействия субъекта на объект могут быть порожденные в ЭС другие субъекты или состояния системы. Как частный случай — это активизация ИУ.

Можно выделить три компонента, связанные с процессом нарушения безопасности систем ИУ [4]:

ИУ — совокупность субъектов и объектов, представляющих нарушителя;

Объект атаки — часть системы, на которую ИУ производит воздействие;

Канал воздействия — физическая среда переноса злоумышленного воздействия.

Под **пользователем** будем понимать один или некоторую совокупность субъектов (S_0), действующих от имени пользователя [3, 5]. Пользователь ЭС, является, таким образом, внешним фактором, управляющим состоянием субъектов. Предполагается, что пользователь не может изменить свойства субъектов доступа. В общем, случае это условие не соответствует реальным системам, в том числе и ЭС, в которых пользователи могут изменять свойства субъектов через изменение программ, программируемых устройств и т.д. Подобная идеализация позволяет построить четкую схему процессов и механизмов доступа, а угрозы безопасности, возникающие вследствие подобных реалий, рассматривать в контексте гарантий выполнения политики разграничения доступа через механизмы неизменности свойств ЭС.

Определим понятие **нарушителя**. В отличие от пользователя, действия нарушителя направлены на нарушение безопасности информации через несанкционированную возможность менять свойства отдельных субъектов и объектов, например, программируемых устройств или активизировать ИУ с помощью субъектов S_0 . Включение такого субъекта в состав системы приводит к тому, что условие неизменности свойства субъектов доступа нарушается. Очевидно, что нарушитель является частным случаем пользователя.

2. МОДЕЛЬ ДОСТУПА В ЭЛЕКТРОННЫХ СИСТЕМАХ

Рассмотрим понятие доступа в ЭС. Понятие доступа является одним из основополагающих в теории защиты информации.

Исходя из этого, центральным положением субъектно-объектной модели является следующее: все процессы безопасности в КС описываются доступами субъектов к объектам, вызывающими потоки информации [2, 3]. Практически, безопасность системы обеспечивается разрешением или запретом доступа для заданных множеств субъектов и объектов. В работе ин-

терпретация понятия доступа в ЭС имеет свои специфические особенности.

В общем случае, механизм доступа (в том числе и несанкционированного), реализуемый субъектом, может быть представлен как выполнение этим субъектом определенных действий над объектом с целью порождения нового субъекта или осуществления обмена информацией между объектами.

Для формализации механизма доступа в субъектно-объектной модели ЭС, воспользуемся следующими определениями [3].

Определение 1. Объект O_i называется источником для субъекта S_k , если существует субъект S_j , в результате воздействия которого на объект O_i в ЭС возникает субъект S_k . Субъект S_k назовем порожденным субъектом.

Определение 2. Субъект S_j , порождающий новый субъект в объекте O_i , в свою очередь, называется активизирующим или порождающим субъектом для субъекта S_k .

Определение 3. Объект O_i в момент времени t ассоциирован с субъектом S_j , если субъект S_j использует информацию, содержащуюся в объекте O_i .

Использование информации можно объяснить, анализируя процедуры взаимодействия субъектов доступа и объектов. Результат показывает, что ассоциированные объекты могут быть разделены на два вида: функционально-ассоциированные объекты и ассоциированные объекты-данные.

Функционально-ассоциированные объекты определяют содержание процедуры воздействия субъекта. Например, микропрограммы в программируемых устройствах определяют свойства субъекта в следующий момент времени. Другой пример, состояние контактов матрицы клавиатуры (замкнуты, разомкнуты) влияет на функции, выполняемые контроллером клавиатуры. Таким образом, матрица клавиатуры является функционально ассоциированным объектом для субъекта — контроллер клавиатуры.

Ассоциированные объекты-данные выступают в роли аргументов в операциях, порождающих потоки информации (например, регистры состояний в устройствах управления).

Множество ассоциированных объектов O_j с субъектом S_i в момент времени t обозначим, как

$$S_i(\{O_j\}t).$$

Активная сущность субъектов доступа заключается в их возможности осуществлять определенные действия над объектами, что объективно приводит к возникновению потоков информации.

Формализуем механизм доступа с целью порождения нового субъекта. Расширим понятие доступа и уточним его модель, приведенную в [4].

Введем операцию:

$$\text{Create}(S_j, O_i, P') \rightarrow S_k, \quad (1)$$

которая означает, что при воздействии субъекта S_j , с помощью активизирующего потока команд P' , на объект O_i порожден субъект S_k . *Create* назовем операцией порождения субъектов.

Отметим, что ввиду того, что в ЭС действует дискретное время, то под воздействием активизирующего субъекта в момент времени t_k , новый субъект порождается в момент времени t_{k+1} .

Результат операции *Create* зависит как от свойств активизирующего субъекта, так и от свойств объекта-источника. В том случае, когда при воздействии субъекта S_j , с помощью активизирующего потока P' , на объект O_i порождение субъекта S_k не происходит $\text{Create}(S_j, O_i, P') \rightarrow \emptyset$.

Если субъект S_j играет роль нарушителя S_0 , а субъект S_k — роль ИУ (S^*), тогда процесс активизации ИУ описывается следующей образом [1]:

$$\text{Create}(S_0, O_i, P'_{unsp}) \rightarrow S^*, \quad (2)$$

где поток P'_{unsp} обозначает поток неспецифицированных команд. Поток P'_{unsp} может быть порожден либо внешним субъектом нарушителя S_0 , либо внутренним механизмом активации ИУ.

Теперь формализуем **механизм доступа с целью реализации обмена информацией** между объектами. По определению, объекты системы являются пассивными сущностями. Для выполнения операции обмена информацией между ними, необходимо существование потоков данных от одного объекта к другому. Приведем определение потока.

Определение 4. Поток информации между объектом O_i и объектом O_j называется операция по обмену данных над объектом O_i , реализуемая субъектом S_k , и зависящая от объекта O_i .

Таким образом, порождение потока информации между объектом O_i (объект-источник) и объектом O_j (объект-получатель) всегда реализуется двумя операциями. Сначала субъект S_j порождает (активизирует) субъект S_k в объекте O_i (1). После этого поток данных P'' от объекта O_i к объекту O_j порождается операцией:

$$\text{Stream}(S_k, O_i, P'') \rightarrow O_j. \quad (3)$$

Stream назовем операцией порождения потока (или обмена информацией между объектами).

Потоки могут создаваться различными типами операций: чтение, изменение, удаление, создание и т. д. Объекты O_i и O_j , участвующие в организации потока, могут быть как источниками, так и приемниками информации, могут быть как ассоциированными, так и неассоциированными с субъектом S_k . Следует особо подчеркнуть, что согласно определению 4, потоки информации могут быть только между объектами, а не между субъектом и объектом. Это объясняется тем, что субъект это активная сущность, т. е. действия, процессы, а информация это пассивная сущность, которая может размещаться,

извлекаться, порождаться, изменяться только в объектах.

Активная роль субъекта заключается в самой реализации потока, через задействование в потоке ассоциированных с субъектом объектов (например, буферов оперативной памяти, регистров). Поток P'' может быть массивом, адресом и т.д.

Подведем итог. Механизм доступа с целью реализации обмена информацией между объектами описывается двумя операциями: операцией порождения субъекта (1) и операцией порождения потока (3):

$$\begin{aligned} \text{Create}(S_j, O_i, P') &\rightarrow S_k, \\ \text{Stream}(S_k, O_i, P'') &\rightarrow O_j. \end{aligned} \quad (4)$$

Предположим, что субъект S_j играет роль нарушителя S_0 , а субъект S_k — роль ИУ S^* , тогда модель несанкционированного доступа с целью реализации обмена информацией между объектами в этом случае, имеет вид:

$$\begin{aligned} \text{Create}(S_0, O_i, P'_{unsp}) &\rightarrow S^*, \\ \text{Stream}(S^*, O_j, P''_{unsp}) &\rightarrow O_m. \end{aligned} \quad (5)$$

Анализируя модель несанкционированного доступа (5) приходим к важному выводу: для обеспечения гарантированного выполнения заданной политики безопасности (ПБ) в ЭС нужно контролировать не только факт несанкционированного доступа субъекта к объекту в виде потоков P'_{unsp} , но и неспецифицированные потоки данных P''_{unsp} .

На основании изложенного, введем определение доступа, которое занимает центральное место в политике и моделях разграничения доступа.

Определение 5. Доступом называется операция обращения субъекта S_k к объекту O_i с целью порождения нового субъекта и/или реализации обмена информацией между объектами O_i и O_j .

Если принять во внимание, что создание субъекта всегда преследует цель выполнения определенных действий над информацией, то можно констатировать, что доступ — это, в общем случае, двухэтапная процедура. Это влечет за собой следующее заключение: модель доступа включает потоки не только между объектами, но и между субъектами и объектами.

Формальное определение доступа (4) дает возможность средствами субъектно-объектной модели перейти непосредственно к описанию процессов безопасности информации в защищенных ЭС.

3. ПОТОКИ И ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА СУБЪЕКТОВ К ОБЪЕКТАМ

Рассмотрим множество потоков P для всей совокупности фиксированных декомпозиций ЭС на субъекты и объекты во все моменты времени. С точки зрения безопасности, трактуемой

как состояние защищенности информации в ЭС, множество потоков P разбивается на два непересекающихся подмножества P_{AU} и P_{UNAU} :

$$P = P_{AU} \cup P_{UNAU},$$

$$P_{AU} \cap P_{UNAU} = \emptyset,$$

где P_{AU} — множество потоков, вызываемых разрешенными (authorized); P_{UNAU} — множество неразрешенных (unauthorized), нарушающих состояние защищенности информации.

Потоки P_{AU} и P_{UNAU} могут быть представлены двумя подмножествами. Так,

$$P_{AU} = P' \cup P'',$$

где P' — специфицированный поток команд, P'' — специфицированный поток данных, а

$$P_{UNAU} = P'_{unsp} \cup P''_{unsp},$$

где P'_{unsp} — несанкционированный поток команд, P''_{unsp} — неспецифицированный поток данных.

На основе множества потоков дается следующее понятие, составляющее основу формализации политики разграничения доступа в моделях безопасности.

Определение 6. Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие множеству P_{AU} .

Это определение является фундаментальным положением субъектно-объектной модели ЭС, на котором будут строиться большинство моделей разграничения доступа, выражающих, собственно, подходы, принципы и механизмы правил разграничения доступа (политику разграничения доступа), а также формальные их спецификации (сами модели разграничения доступа). Ввиду того, что определение 6 не конкретизирует и не детализирует конкретных механизмов фильтрации потоков на санкционированные и несанкционированные, то можно говорить, что субъектно-объектная модель доступа ЭС инвариантна относительно любой принимаемой в ЭС политики безопасности.

4. МОНИТОР БЕЗОПАСНОСТИ ЭС

В данном разделе рассмотрим понятие и роль монитора безопасности ЭС, а также основы построения моделей безопасности схемного уровня.

Анализируя основные положения субъектно-объектной модели системы, касающиеся структуры и функционирования защищенных систем [3], сформулируем аналогичные аксиоматические условия для защищенных ЭС.

Аксиома 1. В защищенной ЭС в любой момент времени любой субъект и объект должны быть идентифицированы и аутентифицированы.

Данная аксиома реализуется самой процедурой проектирования и содержанием процессов функционирования ЭС. Так, для ЭС специфицированные объекты и субъекты, а также топология системы, определяются технической документа-

цией. Аксиома 1 выражает **необходимое условие безопасности (защищенности) информации в ЭС.**

Аксиома 2. В защищенной ЭС должна присутствовать активная компонента (субъект) с соответствующим объектом-источником, которая осуществляет управление доступом и контроль доступа субъектов к объектам.

В [2, 3] для данной активной компоненты утвердился термин «монитор безопасности» (МБ). Это понятие связано с упоминаемой выше задачей фильтрации потоков. Целевая функция МБ — фильтрация потоков с целью обеспечения безопасности ЭС. В защищенной ЭС появляется дополнительная компонента, обеспечивающая управление доступом на основе той или иной политики безопасности.

В виду того, что связи между объектами и субъектами, а также процессы обработки информации устанавливаются на этапе проектирования ЭС, то МБ безопасности должен быть интегрирован непосредственно в систему (в ее ядро) на этапе проектирования. Очевидно, что в рассматриваемом случае МБ реализуется на нулевом (hardware) уровне представления системы и управляет доступом на этом уровне. Наиболее эффективной является стратегия, заключающаяся в такой разработке компонентов ЭС, включая МБ, которая бы изначально строилась на основе определенной модели разграничения доступа.

Таким образом, именно МБ в защищенной ЭС является субъектом осуществления принятой политики безопасности, реализуя ее через алгоритмы своей работы, которые соответствуют модели безопасности. В этом отношении большое значение имеет следующее аксиоматическое положение [3], расширенное для случая ЭС.

Следствие 1 (из аксиомы 2). В защищенной ЭС существует особая категория субъектов (активных сущностей), которые не инициализируют другие субъекты и к которым отсутствует доступ пользователя (нарушителя).

Это системные субъекты (процессы), присутствующие (функционирующие) в системе изначально. К числу подобных системных субъектов относится МБ, который управляет доступами субъектов (в том числе и пользователей) к объектам системы. Следовательно, для обеспечения защищенности в ЭС свойства системных субъектов должны быть неизменными, от чего напрямую зависят гарантии безопасности.

Аксиома 3. Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам необходима (должна существовать) дополнительная информация и объекты, ее содержащие.

Из аксиомы 3 следует, что МБ, в свою очередь, как и любая активная сущность в ЭС, является субъектом с соответствующим объектом-источником и ассоциированными объектами. Отсюда вытекают следующие важные следствия.

Следствие 2 (из аксиомы 3). Ассоциированный с монитором безопасности объект, содержащий информацию о системе разграничения доступа, является наиболее критическим с точки зрения безопасности информационных ресурсов в защищенной ЭС.

Действительно возможность несанкционированно изменять, удалять данный объект может полностью разрушить или сделать не эффективной всю систему безопасности ЭС. Поэтому способы и особенности реализации данного объекта имеют определяющее значение для защищенности информации в ЭС.

Информация в ассоциированном с монитором безопасности объекте должна касаться специфицированных субъектов и объектов системы, а также топологии системы. Следовательно, для планирования и управления системой разграничения доступа ЭС должна быть предусмотрена процедура доступа к данному объекту со стороны внешней среды, т. е. через субъекты пользователя. Отсюда вытекает еще одно следствие.

Следствие 3 (из аксиомы 3). В защищенной системе может существовать **доверенный пользователь (системный администратор)**, субъекты которого имеют доступ только к ассоциированному с монитором безопасности объекту для управления политикой разграничения доступа. Эти субъекты не должны иметь доступ к элементам или процессам монитора безопасности.

Принципы, способы представления и реализация ассоциированных с монитором безопасности объектов определяются типом политики безопасности и особенностями конкретной ЭС.

В практическом плане, к реализации монитора безопасности ЭС, предъявляются следующие обязательные требования:

1. Полнота. МБ должен вызываться (активизироваться) при каждом обращении за доступом любого субъекта к любому объекту, и не должно быть никаких способов его обхода.

2. Если предположить, что ИУ может воспользоваться штатным каналом ЭС, т.е. каналом, который поддерживает потоки из множества P_{AU} , становится очевидным необходимость осуществления контроля всех потоков в каналах связи.

3. Изолированность. МБ должен быть защищен от отслеживания и перехвата своей работы.

4. Верифицируемость. МБ должен быть проверяемым (само- или внешне тестируемым) на предмет выполнения своих функций.

5. Непрерывность. МБ должен функционировать при любых штатных и нештатных, в том числе и аварийных ситуациях.

6. Механизм управления доступом должен гарантированно реализовывать заданную политику безопасности.

7. Механизм управления доступом не должен влиять на качество выполнения ЭС основных функций.

Включение в архитектуру ЭС специального субъекта для мониторинга должно обеспечивать конфиденциальность, целостность и доступность информации.

5. ОБЕСПЕЧЕНИЕ ГАРАНТИЙ ПОЛИТИКИ БЕЗОПАСНОСТИ ЭС

Целью данного подраздела является разработка критериев гарантированной безопасности ЭС.

Как правило, модели, связанные с реализацией политики безопасности [2, 5, 6], не учитывают возможности субъектов по изменению самой системы, которые могут привести к изменению её свойств, и как предельный случай, к полной неприменимости той или иной модели к описанию отношений «субъект-объект» уже в измененной системе. Поэтому вопрос гарантий политики безопасности является ключевым как в теории, так и в практике.

Рассматривая активную роль субъектов (в том числе и ИУ) в ЭС, необходимо отметить ряд важнейших их свойств, на которых базируются излагаемые ниже гарантии безопасности.

Во-первых, необходимо заметить, что человек-пользователь воспринимает объекты и получает информацию о состоянии ЭС через субъекты, которыми он управляет и которые производят отображение информации в воспринимаемом человеком виде.

Во-вторых, угрозы компонентам ЭС исходят от субъектов как активной компоненты, порождающей потоки и изменяющей состояние объектов в КС.

В-третьих, субъекты могут влиять друг на друга через изменяемые ими объекты, связанные с другими субъектами, порождая в конечном итоге в системе субъекты (или состояния системы), которые представляют угрозу для безопасности информации или для работоспособности самой системы

В-четвертых, субъекты, которые представляют угрозу для безопасности информации, могут использовать штатные каналы системы.

Положения субъектно-объектной модели системы, а также, понятия доступа субъектов к объектам и политики безопасности позволяют сформулировать следующий общий критерий безопасности системы [2, 3].

Определение 7. Электронная система безопасна тогда и только тогда, когда субъекты не имеют никаких возможностей нарушать (обходить) установленную в системе политику безопасности.

Субъектом обеспечения политики безопасности выступает монитор безопасности (МБ). Его наличие в структуре ЭС является необходимым условием безопасности. Что касается условий достаточности, то, очевидно, они заключены, несмотря на тавтологию выражения, прежде всего, в безопасности самого МБ.

В практической реализации выполнение данного требования, с учетом определения доступа, приводит к необходимости разделения МБ на два отдельных субъекта: монитор безопасности объектов (МБО); монитор безопасности субъектов (МБС). Введем соответствующие определения.

Определение 8. Монитором безопасности объектов называется субъект, активизирующийся при возникновении потока, порождаемого любым субъектом, между любыми объектами и разрешающий только те потоки, которые принадлежат множеству P'' . МБО должен фильтровать те потоки, которые принадлежат множеству P''_{unsp} .

Определение 8, по сути, вводит в состав политики безопасности ЭС, в качестве дополнительной составной части, специальную политику относительно потоков информации между объектами.

Определение 9. Монитором безопасности субъектов называется субъект, активизирующийся при любом порождении субъектов, и разрешающий порождение субъектов из фиксированного подмножества пар активизирующих субъектов и объектов-источников.

МБС разрешает только те потоки, которые принадлежат множеству P' . МБС должен фильтровать те потоки, которые принадлежат множеству P'_{unsp} .

Определение 9, практически, вводит в состав политики безопасности ЭС в качестве дополнительной составной части специальную политику относительно порождения субъектов доступа.

Как и у любого субъекта, у МБС должен быть объект-источник, функционально-ассоциированный объект, включающий, например, программируемый модуль и ассоциированный объект-данные, содержащий необходимую информацию по политике порождения субъектов доступа в системе (рис. 1).

Атаки некоторых типов ИУ [1,7] осуществляются по сценарию подмены функций специфицированных субъектов (т. е. фактически

подмены свойств субъектов) или возникновения нового неспецифицированного субъекта. Поэтому важным аспектом, с точки зрения гарантий выполнения политики безопасности, является **неизменность свойств субъектов** доступа в процессе функционирования ЭС. Данное требование имеет отношение к любым субъектам доступа, но особо для субъектов МБ.

Для построения доказательной базы защищенности информации в ЭС рассмотрим следующие понятия: тождественность объектов, а также тождественность и неизменность субъектов.

Определение 7. Объекты O_i и O_j в момент времени t тождественны ($O_i(t) \equiv O_j(t)$), если они совпадают как структура, так и как слова, записанные в одном языке в памяти.

В частном случае, когда ($O_i(t_1) \equiv O_j(t_2)$) $t_1 \neq t_2$, будем говорить о тождественности одного и того же объекта в разные моменты времени.

Тождественность объектов по определению 7 основывается как на физической (структурной) тождественности, так и на тождественности уровня последовательности символов из алфавита языка представления [3, 5]. Введенное понятие тождественности объектов позволяет перейти к рассмотрению понятия тождественности и неизменности субъектов доступа.

Определение 8. Субъекты S_i и S_j тождественны в момент времени t , если попарно тождественны все ассоциированные с ними объекты.

В общем случае, определения 7 и 8 неявно требуют наличия в системе специального механизма сортировки однотипных объектов и их попарного сравнения. В электронных системах тождественность объектов, а также тождественность и неизменность субъектов выполняются априорно за счет неизменности электрических соединений и функциональной спецификации, реализованной на этапе проектирования. Это обуславливает следующее следствие.

Следствие 4 (из определений 7 и 8). В электронных системах тождественность объектов, а также тождественность и неизменность субъек-

Защищенная ЭС

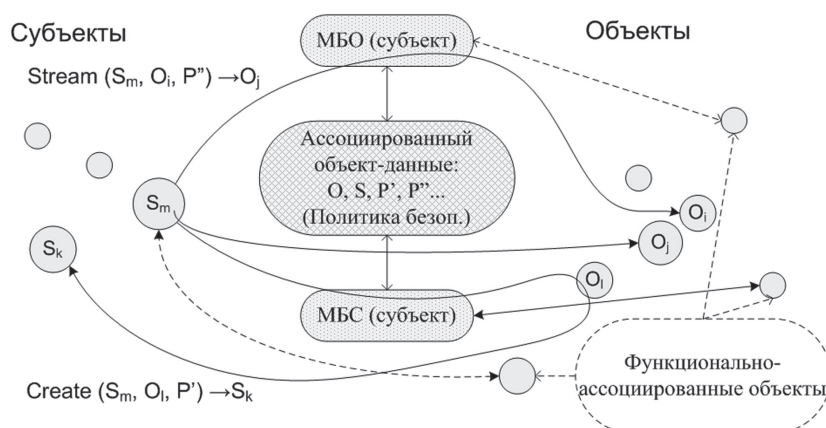


Рис. 1. Порождение потоков (Stream) и субъектов (Create) с учетом МБО и МБС

тов обеспечивается фильтрацией (блокировкой) потоков P'_{unsp} .

Рассмотрим объект O_i , который содержит ИУ. Сравним этот объект O_i в момент времени t , когда ИУ находится в пассивном состоянии, с этим же объектом O_i в момент времени $t+1$, когда ИУ находится в активном состоянии. Будучи физически тождественными в момент времени t , эти объекты стали физически не тождественными после активизации ИУ в момент времени $t+1$. Сделаем вывод: отсутствие потока P'_{unsp} в момент времени t гарантирует тождественность объектов в момент времени $t+1$, а, следовательно, гарантирует отсутствие угроз, исходящих от ИУ, и появление потоков P''_{unsp} . Исключением является случай автономной активизации или активизации с помощью беспроводного канала.

Следствие 5 (из определений 7 и 8). Порожденные субъекты тождественны, если тождественны все порождающие субъекты и объекты-источники.

Обоснованность данного следствия вытекает из тождественности функционально-ассоциированных объектов в порождающих субъектах, которые отвечают за порождение нового субъекта, а также из тождественности аргументов операции порождения, т. е. ассоциированных объектов-данных и объектов-источников, которые определяют свойства порождаемых субъектов. Очевидно, что субъекты, осуществляющие доступ к объектам системы, в том числе и к объектам, ассоциированным с другими субъектами, могут тем самым влиять на них и изменять их свойства. Поэтому вводится следующее определение.

Определение 9. Субъекты S_i и S_j называются не влияющими друг на друга (или корректными относительно друг друга), если в любой момент времени отсутствует поток (изменяющий состояние объекта) между любыми объектами O_i и O_j , ассоциированными, соответственно с субъектами S_i и S_j . Причем объекты O_i не ассоциированы с субъектом S_j , а объекты O_j не ассоциированы с субъектом S_i .

Отметим, что термин «изменение состояния объекта» в определении 9 трактуется как нетождественность (в смысле определения 7) объекта с самим собой в различные моменты времени. При этом подчеркивается, что операция изменения объекта локализована в субъекте, с которым этот субъект не ассоциирован. Очевидно, что в ЭС эта нетождественность порождается потоками P'_{unsp} или P''_{unsp} .

Анализ понятия ассоциированных с субъектом объектов позволяет ввести еще более жесткое определение по влиянию одних субъектов на других.

Определение 10. Субъекты S_i и S_j называются абсолютно не влияющими друг на друга (или абсолютно корректными относительно друг друга), если в условиях определения 9 множества ассо-

циированных объектов указанных субъектов не имеют пересечения.

На основании данного определения можно сформулировать достаточное условие гарантированного выполнения политики безопасности.

Утверждение 1 (достаточное условие гарантий безопасности 1). Монитор безопасности объектов разрешает порождение потоков только из множества P'' , если все существующие в системе субъекты абсолютно корректны относительно него и друг друга.

Доказательство. Из условия абсолютной корректности любых субъектов с МБО вытекает отсутствие потоков P''_{unsp} , которые могут изменить функционально-ассоциированные и ассоциированные объекты-данные МБО и тем самым изменить его свойства для осуществления обхода (нарушения) политики безопасности.

С другой стороны, такие потоки могут появиться при изменении ассоциированных объектов, принадлежащих другим субъектам ЭС для возможного нарушения (обхода) политики безопасности. Условие корректности субъектов относительно друг друга делает это невозможным (по определению абсолютной корректности). Это в свою очередь означает, что МБО реализует только потоки из множества P'' . Тем самым **утверждение доказано**.

Утверждение 1 для обеспечения гарантий безопасности накладывает чрезвычайно жесткие и труднореализуемые на практике условия. Кроме того, невозможно гарантировать корректность любого субъекта, активизируемого в ЭС (особенно в случае автономной активизации ИУ), относительно МБО. Очевидно, что эти условия существенно снижают функциональные возможности ЭС (фактически, это требование отсутствия общих ассоциированных объектов-данных, например, регистров состояния, буферов для обмена данными, а также ассоциированных объектов источников, например, МП для субъектов).

С практической точки зрения, наиболее логичными и интересными являются подходы, позволяющие уменьшить число объектов и субъектов, которые охватываются политикой безопасности. При проектировании ЭС всегда можно гарантированно обеспечить сокращение множества возможных порождаемых субъектов до некоторого подмножества фиксированной мощности, при этом, не гарантируя отсутствия некорректных субъектов внутри этого подмножества.

Отметим, что в сформированное подмножество субъектов в момент времени t включается и МБС. Поэтому, первым аргументом операции Create может быть только субъект, входящий в подмножество субъектов, а аргумент-объект, вообще говоря, любым.

Для демонстрации этого подхода введем понятия замкнутости и изолированности подмножества субъектов системы.

Определение 11. ЭС называется замкнутой по порождению субъектов, если в ней действует МБС, разрешающий порождение только фиксированного конечного подмножества субъектов для любых объектов-источников, рассматриваемых для фиксированной декомпозиции ЭС на субъекты и объекты.

Согласно этому определению подмножество субъектов может включать некорректные субъекты, т.к. объекты-источники могут быть и не нетождественными относительно друг друга.

Для описания системы в части защищенности, свойство замкнутости ЭС по порождению субъектов необходимо дополнить свойством изолированности.

Определение 12. Множество субъектов ЭС называется изолированным (абсолютно изолированным), если в ней действует МБС и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и МБС.

Таким образом, механизм замкнутой по порождению субъектов ЭС и свойство изолированности множества субъектов сокращает множество возможных порождаемых субъектов до некоторого подмножества фиксированной мощности, при этом, не гарантируя отсутствия некорректных субъектов внутри замкнутой среды.

Из определения 12 вытекают следующие следствия.

Следствие 6 (из определения 12). Любое подмножество субъектов изолированной (абсолютно изолированной) ЭС, включающее МБС, также составляет изолированную (абсолютно изолированную) среду.

Следствие 7 (из определения 12). Дополнение изолированной (абсолютно изолированной) среды субъектом, корректным (абсолютно корректным) относительно любого субъекта из числа входящих в изолированную (абсолютно изолированную) среду, оставляет ее изолированной (абсолютно изолированной).

На этой основе можно сформулировать другое условие достаточности гарантий выполнения политики безопасности.

Утверждение 2 (достаточное условие гарантий безопасности 2). Если в абсолютно изолированной ЭС существует МБО и порождаемые субъекты абсолютно корректны относительно МБО, а также существует МБС, который абсолютно корректен относительно МБО, то в ЭС реализуется только доступ, описанный политикой разграничения доступа.

Доказательство. По определению 12 и следствиям из него в системе могут существовать только абсолютно корректные относительно МБС и друг друга субъекты из некоторого их конечного множества. Следовательно, отсутствует возможность изменения свойств МБС. Абсолютная корректность МБС и других субъектов по отношению к МБО обеспечивает отсут-

ствие возможностей изменения свойств МБО, что в итоге автоматически обеспечивает разрешение только тех потоков, которые входят в множество $P_{AU} = P' \cup P''$. Утверждение доказано.

В отличие от первого условия достаточности гарантий выполнения политики безопасности, когда требовалась корректность МБО относительно произвольного субъекта, второе условие менее жестко, т. к. накладывает условия абсолютной корректности не на все множество возможных субъектов, а лишь на фиксированное их подмножество, образующее замкнутую аппаратную среду. И все же, требование абсолютной корректности, хотя и для фиксированного подмножества субъектов, является также чрезвычайно жестким и трудно выполнимым на практике без существенного снижения функциональных возможностей КС.

Дальнейший анализ подходов к гарантиям безопасности, точнее, к возможностям реализации изолированной ЭС, показал необходимость включения требований по неизменности свойств объектов, связанных с процедурами порождения субъектов.

При технической реализации операции Create по порождению субъектов, которые составляют изолированную среду в ЭС, возникает весьма важная проблема, связанная с тем, что в реальной ЭС один и тот же объект может иметь различные состояния во времени (например, безопасные или опасные). Предположим, что зафиксировано состояние объекта O_i в некоторый момент времени t_0 . Обозначим состояние объекта O_i в момент времени t как $O_i(t)$.

Определение 13. Операция порождения субъектов $Create(S_j, O_i, P) \rightarrow S_k$, называется порождением с контролем неизменности объекта, если для любого момента времени $t > t_0$, в который активизирована операция порождения субъекта Create, порождение субъекта S_k возможно только при тождественности объекта-источника относительно момента t_0 , т. е. при $O_m(t) \equiv O_m(t_0)$.

Из определения 13 вытекает следующее важное следствие, имеющее непосредственное отношение к неизменности свойств субъектов доступа, как важнейшего условия обеспечения политики безопасности в системе.

Следствие 8 (из определения 13). В условиях определения 13 порожденные субъекты $S_i(t_1)$ и $S_i(t_2)$ тождественны, если $t_1 > t_0$ и $t_2 > t_0$. При $t_1 = t_2$ порождается один и тот же субъект.

Введение понятия порождения субъектов с контролем неизменности объектов позволяет сформулировать и доказать такое достаточное условие для обеспечения замкнутой ЭС, которое во-первых, может быть практически реализовано в реальных ЭС, а во-вторых, сделать безопасной траекторию состояний ЭС.

Утверждение 3. (базовая теорема изолированной ЭС). Если в момент времени t_0 в изолированной ЭС действует только порождение

субъектов с контролем неизменности объекта, и существуют потоки от любого субъекта к любому объекту, не противоречащие условию корректности (абсолютной корректности) субъектов, то в любой момент времени $t > t_0$ ЭС также остается изолированной (абсолютно изолированной).

Доказательство. Условие корректности для потоков в начальный момент t_0 времени функционирования системы обеспечивает исходную «безопасность» всех объектов-источников для последующего порождения субъектов системы, порождением с контролем неизменности объекта.

По условию утверждения 3 в ЭС возможно существование потоков, изменяющих состояние объектов, не ассоциированных в этот момент времени с каким-либо субъектом. Если объект с измененным состоянием не является источником для порождения субъекта, то множество субъектов изолированной среды нерасширяемо, в противном случае (измененный объект является источником для порождения субъекта с нарушением условия «контроля неизменности объекта») по условиям утверждения (порождение субъекта с контролем) порождение субъекта невозможно. Следовательно, мощность множества субъектов не может превышать той, которая была зафиксирована до изменения состояния любого объекта. Таки образом, множество субъектов ЭС остается изолированным и любой момент времени будут соблюдаться требования изолированности ЭС. Утверждение доказано.

ВЫВОДЫ

1. Утверждения 1–3 имеют важное значение с точки зрения достаточных условий для обеспечения гарантий выполнения политики безопасности в защищенных ЭС, т.к. позволяют сформулировать методологию проектирования гарантировано защищенных ЭС.

2. Теоретические результаты, полученные в работе, создают **инвариантную основу** по отношению к любым политикам и моделям разграничения доступа для гарантий выполнения политики безопасности в защищенных ЭС.

3. Вместе с тем, не рассмотрена ситуация, связанная с автономной активацией ИУ и активацией с помощью беспроводного канала.

4. При практической реализации условий утверждения 3 возникает несколько серьезных проблем. Одна из них связана с исходным состоянием ЭС, в котором должны быть только потоки, гарантирующие корректность исходных субъектов. Вторая проблема связана с понижением производительности (быстродействия) ЭС в связи с выполнением процедур контроля мониторингом безопасности.

Литература

- [1] Горбачев В.А. Иванисенко И.Н. Классификация и формальные модели аппаратных закладных устройств. Прикладна радіоелектроніка та інформатика, Харьков: ХТУРЭ. — Т. 6, 2007. № 2. — С. 306–310.
- [2] Bishop M. Computer Security: art and science. Addison Wesley.
- [3] Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Уральский государственный университет им. А.М. Горького, Екатеринбург, 2008.
- [4] Горбачев В.А. Формальные основы методов блокирования аппаратных закладных устройств// Прикладна радіоелектроніка, науч.-техн. журнал, Харьков: ХНУРЭ. — Т. 11, 2012. № 2. — С. 275–280.
- [5] Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. — М.: Изд. центр «Академия», 2005. — 144 с.
- [6] Зегжда Д.П., Иващенко А.М. Основы безопасности информационных систем — М.: Телеком, 2000. — 452 с.
- [7] Benjamin Sanno, Detecting Hardware Trojans, Matrikelnummer: 108006248774 benjamin.sanno@rub.de Semester 6 Ruhr-University Bochum, Germany July 22, 2009.



Поступила в редколлегию 3.06.2014

Горбачев Валерий Александрович, профессор кафедры ЭВМ ХНУРЭ. Научные интересы: системный анализ.

УДК 638.235.231

Достатні умови безпеки інформації в електронних системах / В.О. Горбачов // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 319–327.

Розглядається суб'єктно-об'єктна модель доступу, аксіоматичні достатні умови захищеності інформації, а також вимоги до монітора безпеки в електронних системах.

Ключові слова: політика безпеки, модель доступу, розмежування доступу, монітор безпеки, електронна система.

Лл.: 1. Бібліогр.: 7 найм.

UDC 638.235.231

Sufficient conditions of information security in electronic systems / V.A. Gorbachov // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 319–327.

A subject-object access model, axiomatic sufficient conditions of information security as well as requirements specified to security monitors in electronic systems are considered.

Keywords: security policy, access model, access isolation, security monitor, electronic system.

Fig. 1. Ref.: 7 items.

МЕТОД ПРОЕКТУВАННЯ ТА ВЕРИФІКАЦІЇ ФУНКЦІЙ КОМПЛЕКСІВ ЗАСОБІВ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

А.В. ЛЄНШИН

Пропонується комплексний метод проектування та верифікації комплексів засобів захисту інформації від несанкціонованого доступу. Аналізується підхід щодо створення та використання шаблонів для алгоритмів реалізації послуг безпеки у формальній нотації Паронджанова. Наводиться приклад застосування методу для розробки алгоритму реалізації послуги «відновлення після збоїв».

Ключові слова: захист від несанкціонованого доступу, НД ТЗІ 2.5-004-99, системний аналіз, дракон-схеми, нотація Паронджанова.

ВСТУП

Захист інформації, що обробляється в інформаційно-телекомунікаційних системах (ІТС), є завданням, що має вирішуватися за рахунок комплексного підходу, який передбачає застосування узгодженої сукупності процедурних, адміністративних та програмно-технічних рішень.

У разі створення комплексних систем захисту інформації (обов'язкова вимога законодавства у разі обробки в ІТС інформації з обмеженим доступом та/або інформації, яка відноситься до державних інформаційних ресурсів) мають використовуватися засоби технічного захисту інформації (ТЗІ): програмні, апаратні, апаратно-програмні.

Проектування комплексу засобів захисту (КЗЗ), що реалізовані у засобах ТЗІ, які використовуватимуться в складі КСЗІ, має здійснюватися з використанням критеріїв захищеності, що визначені у НД ТЗІ 2.5-004-99 [1].

Аналіз нормативної бази та сучасних публікацій вказує на відсутність методу, який би дозволяв здійснювати проектування КЗЗ від несанкціонованого доступу (НСД) із заданим рівнем гарантій та можливостями щодо протидії наперед визначеній множині загроз. На думку автора, особливо корисним цей метод має стати для розробників захищених від НСД компонентів обчислювальної системи, в яких функції захисту є додатком до основних — «бізнес» функцій продукту.

1. СУТНІСТЬ МЕТОДУ ПРОЕКТУВАННЯ ТА ВЕРИФІКАЦІЇ ФУНКЦІЙ КЗЗ ВІД НСД

Послідовність дій запропонованого у роботі методу згруповано у три етапи: «підготовка», «проектування» та «верифікація».

Дії, які виконуються на етапі «підготовка» здійснюються лише у ході розробки/адаптації метода, при цьому основними кроками етапу є:

- визначення набору критеріїв оцінки захищеності від НСД;
- первинна формалізація вимог критеріїв за рахунок структуризації їх вимог у вигляді множинних описів;
- розробка шаблонів для алгоритмів реалізації послуг безпеки при функціонуванні КЗЗ;

— визначення «типової» множини загроз безпеки, яким здатний протидіяти КЗЗ, спроектований за обраними критеріями [2];

— розробка правил уточнення множини загроз на етапі «проектування»;

— розробка правил формування програми випробувань із заданим рівнем покриття;

— визначення правил (функції) відображення множин загроз/послуг безпеки.

Виконання дій етапу «проектування» покладаються безпосередньо на розробника КЗЗ чи захищеного від НСД компонента обчислювальної системи, при цьому основними кроками етапу є:

— вибір (уточнення) підмножини загроз, яким має протидіяти КЗЗ розроблюваного засобу;

— відображення обраної множини загроз до переліку послуг безпеки;

— заповнення шаблонів послуг безпеки.

Дії, які виконуються на етапі «верифікація», можуть здійснюватися як у ході проведення попередніх випробувань, що проводяться розробником, так і під час проведення сертифікаційних випробувань (в Україні такими випробуваннями слід вважати Державну експертизу у сфері ТЗІ).

Основними кроками етапу «верифікація» є:

— формування програми випробувань за правилами, що є частиною методу;

— корегування типової методики випробувань з урахуванням особливостей КЗЗ, що розробляється;

— проведення випробувань та формування пропозицій з усунення викритих недоліків.

Окремо слід підкреслити, що в ході використання методу «автоматично» задовольняються умови, необхідні для забезпечення заданого рівня гарантій [1, 3].

2. ШАБЛони ДЛЯ АЛГОРИТМІВ РЕАЛІЗАЦІЇ ПОСЛУГ БЕЗПЕКИ ПРИ ФУНКЦІОНУВАННІ КЗЗ

Практичне застосування НД ТЗІ 2.5-004-99 під час розробки та експертизи КЗЗ свідчить, що форма подання специфікацій послуг є ускладненою і нечіткою [2]. Це призводить до неоднозначності у розумінні вимог розробниками КЗЗ та не лише негативно впливає на рівень захисту,

але і зумовлює додаткові фінансові витрати на усунення недоліків, викритих державними експертами з ТЗІ.

Зазначену проблему, у рамках застосування методу, пропонується вирішувати за рахунок розроблення шаблонів для алгоритмів реалізації послуг безпеки при функціонуванні КЗЗ. Шаблони є формалізованим поданням вимог нормативних документів, що регламентують порядок захисту від загроз НСД. В ході застосування такого підходу від розробника КЗЗ вимагається лише заповнити змінювані параметри залежно від особливостей продукту (середовища користувачів, технології обробки інформації, середовища використання тощо).

На основі висунутих критеріїв вибору способу опису алгоритмів, а саме: можливість формалізованого подання та наочність відображення, було обрано нотацію, яка запропонована Володимиром Паронджановим (відома під назвою: візуальна мова «Дракон») [4].

Обрана нотація базується на основі застосування двовимірних інформаційних оптичних сцен (діосцен). Для подання алгоритмів використовується множина ікон (дія, вибір, питання, адреса, петля циклу, петля силуету, вставка тощо) та макроікон (розвилка, перемикачі, цикл з передумовою, цикл з післяумовою тощо).

Застосування нотації Паронджанова та доступних у мережі Інтернет засобів розробки дозволяють автоматично генерувати вихідні програмні коди мовами програмування (C, C++,

Object Pascal, Assembler), з яких без додаткових зусиль можна отримати код, що виконується, із застосуванням стандартних компіляторів.

Незаперечною перевагою застосування нотації Паронджанова є наочність відображення алгоритмів та повністю формальне подання правил візуального структурного програмування.

На рис. 1 подано шаблон алгоритму реалізації послуги КА-2 «Базова адміністративна конфіденційність» у нотації Паронджанова (схема типу «Силует»). Окремо підкреслимо, що ідеологічною особливістю нотації Паронджанова є застосування носіїв подання інформації великого формату. Враховуючи обмеження сторінки збірника, на рисунку використані позначення (табл. 1), що погіршують ергономічний ефект від застосування нотації. Зацікавлений користувач зможе змодельовати приклад, використовуючи вільно доступні в мережі Інтернет засоби [5].

3. ПРИКЛАД ЗАСТОСУВАННЯ МЕТОДУ ДЛЯ ПРОЕКТУВАННЯ ФУНКЦІЙ КЗЗ, ЩО РЕАЛІЗУЄ ПОСЛУГУ ВІДНОВЛЕННЯ ПІСЛЯ ЗБОЇВ

Фахівці у сфері захисту інформації сходяться на думці, що однією із особливостей, яка зумовлена впровадженням інформаційних технологій у повсякденну діяльність людини, є зміщення акцентів із забезпечення конфіденційності інформації на підтримку безперервності роботи бізнесу. Враховуючи слабкість «людського чинника» цілком зрозумілим є прагнення розробни-

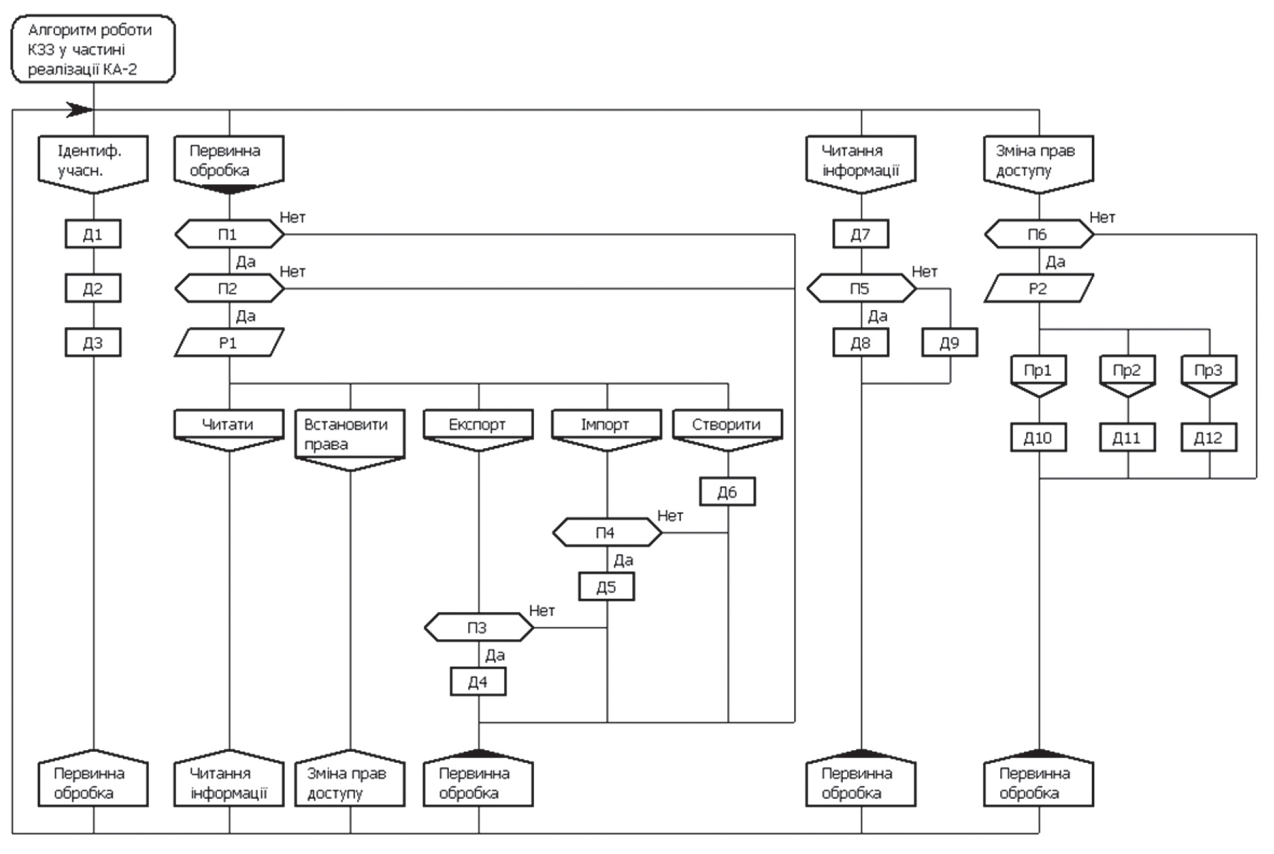


Рис. 1. Шаблон для алгоритму реалізації послуги КА-2

Таблиця 1

Використані на схемі позначення

Поз.	Розшифровка позначення
Д1	Визначити атрибути доступу для Користувача
Д2	Визначити атрибути доступу для Об'єкта
Д3	Визначити атрибути доступу для Процесу
Д4	Встановити для Об'єкта права доступу, що визначені політикою та виконати експорт
Д5	Виконати імпорт та встановити для Об'єкта права доступу, що визначені політикою
Д6	Створити новий об'єкт із правами доступу, що визначені політикою за замовчуванням
Д7	Зчитати матрицю доступу Користувачі/Об'єкти
Д8	Дозволити Користувачу прочитати вміст Об'єкта
Д9	Відмовити Користувачу у читанні вмісту Об'єкта
Д10	Змінити атрибути користувачів
Д11	Змінити атрибути захищених об'єктів
Д12	Змінити права на ініціювання процесів
П1	Чи має Користувач і/або групи до яких він входить право ініціювати Процес?
П2	Чи входить Об'єкт до множини об'єктів, для яких здійснюється розмежування доступу на читання?
П3	Чи має Користувач право на експорт?
П4	Чи має Користувач право на імпорт?
П5	Чи дозволено згідно з матрицею доступу читання вмісту Об'єкта для Користувача і/або групи до яких він входить?
П6	Чи є користувач уповноваженим користувачем?
Р1	Який тип має Запит?
Р2	Який підтип Запиту?
Пр1	Запит на зміну атрибутів доступу користувачів
Пр2	Запит на зміну атрибутів доступу об'єктів
Пр3	Запит на зміну атрибутів ініціації процесу

ків програмного та апаратного забезпечення до хоча б часткової автоматизації задач відновлення.

У нормативних документах з ТЗІ [1] закріплено послугу безпеки «відновлення після збоїв», що складається з трьох ієрархічно пов'язаних сукупностей вимог (рівнів):

- ручне відновлення (ДВ-1);
- автоматизоване відновлення (ДВ-2);
- вибіркове відновлення (ДВ-3).

Враховуючи те, що відмови та переривання в обслуговуванні можуть бути зумовлені як реалізацією об'єктивних, так і суб'єктивних загроз, обов'язковим елементом специфікації послуг «Відновлення після збоїв» є така вимога:

«Після відмови або переривання обслуговування КЗЗ повинен перевести комп'ютерну систему до стану, із якого повернути її до нормального функціонування може тільки адміністратор».

Результати проектування «окремого» варіанта реалізації послуги «Відновлення після збоїв», що використовує механізми захисту ОС

Windows, який розроблений на основі шаблону для послуги ДВ-1, наведено на рис. 2. Розглянемо його зміст детальніше.

Аналіз способів реалізації зазначених послуг у засобах ТЗІ, що мають позитивні експертні висновки Адміністрації Держспецзв'язку показав, що послуга ДВ найчастіше реалізується у системах, що мають трирівневу архітектуру або мають змогу працювати у привілейованому режимі (режимі ядра). Такі системи мають характерну ознаку: функціонування захищеного компонента в окремому домені виконання. Переважна більшість програм, для яких необхідно створити КЗЗ, не використовують драйвери та не працюють у режимі ядра. При цьому, міркування безпеки вимагають запускати ці програми від облікового запису з обмеженими правами.

Застосування шаблону для алгоритму реалізації послуги дозволило запропонувати альтернативний розв'язок зазначеної проблеми за рахунок висунення припущень щодо середовища використання продукту: *«При інсталяції програмного забезпечення адміністратором мають бути здійснені налаштування, що забезпечать реалізацію заданої політики розмежування доступу (ПРД) до об'єктів, що зберігатимуть еталонну інформацію щодо стану об'єкта захисту».*

ПРД до об'єктів, які зберігатимуть еталону інформацію подамо у вигляді таких правил:

— КЗЗ повинен мати право записувати та читати інформацію, що пов'язана з подіями безпеки;

— користувач, від імені якого запущено програму, не повинен мати право на зміну еталонної інформації.

Відомо, що для окремих категорій об'єктів, які підлягають захисту (каталоги, файли, елементи реєстру), механізми операційних систем з лінійки Windows дозволяють розділити право на запис та право на дописування інформації. Скориставшись цим у процесі інсталяції, можна призначити права доступу (засобами Windows) до файла (який буде сховищем еталонної інформації), що дозволять реалізувати задану політику розмежування доступу.

ВИСНОВКИ

Розроблений метод за рахунок використання методів системного аналізу при формалізації та верифікації вимог із захисту від НСД та застосування нотації Володимира Паронджанова (схеми типу «Силует») для опису шаблонів та алгоритмів функціонування КЗЗ дозволяє:

- розробити шаблони для алгоритмів реалізації послуг безпеки при функціонуванні КЗЗ;
- генерувати код програмних продуктів;
- задовольняти вимоги гарантій рівня Г-3;
- проводити випробування КЗЗ із наперед-визначеним ступенем покриття.

Подальшим завданням є розробка програмного засобу проектування КЗЗ на основні запропонованого методу.

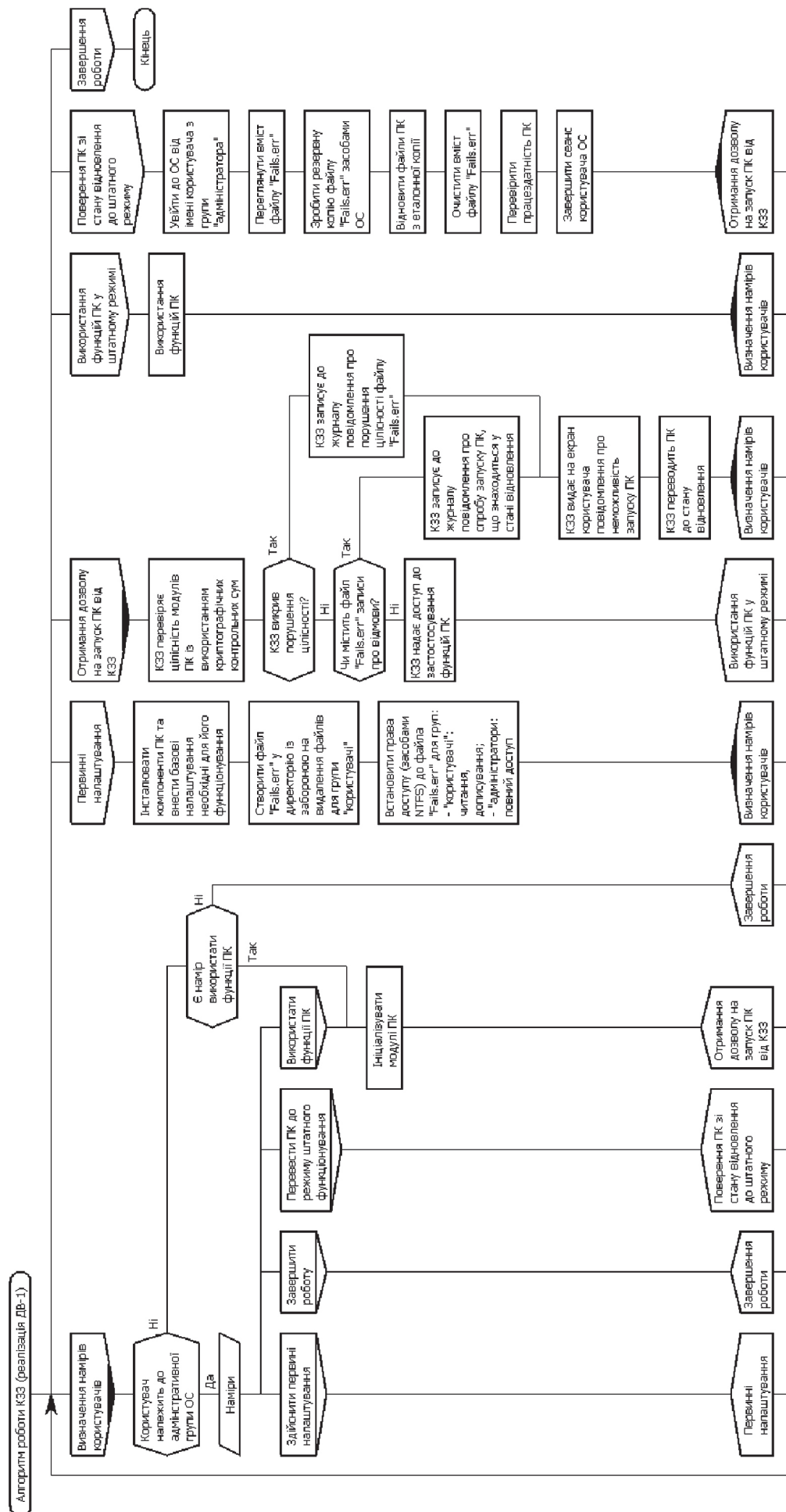


Рис. 2. Алгоритм роботи КЗЗ в ході реалізації послуги ДВ-1

Література

- [1] НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від НСД.
- [2] Леншин А.В. Метод формування функціональних профілів захищеності від несанкціонованого доступу / А.В. Леншин, П.В. Буслов // Науково-технічний журнал "Радіоелектронні і комп'ютерні системи". — Харків: ХАІ, 2010— Том 7. — С. 77—81.
- [3] ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.
- [4] Паронджанов В. Дружелюбные алгоритмы, понятные каждому. Как улучшить работу ума без лишних хлопот — М.: ДМК Пресс, 2010. — 466 с.
- [5] <http://drakon-practic.ru/>

Надійшла до редколегії 18.06.2014



Леншин Анатолій Валерійович, кандидат технічних наук, доцент, докторант кафедри «БІТ» ХНУРЕ. Наукові інтереси: захист від НСД, захист персональних даних, управління інформаційною безпекою.

УДК 681.3.06

Метод проектирования и верификации функций комплексов средств защиты от несанкционированного доступа / А.В. Леншин // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 328—332.

Предлагается комплексный метод к проектированию и верификации комплексов средств защиты информации от НСД. Анализируется подход к созданию и использованию шаблонов для алгоритмов реализации услуг безопасности в формальной нотации Паронджанова. Приводится пример применения метода для разработки алгоритма реализации услуги «восстановление после сбоя».

Ключевые слова: защита от несанкционированного доступа, НД ТЗИ 2.5-004-99, системный анализ, дракон-схемы, нотация Паронджанова.

Табл.: 01. Ил.: 02. Библиогр.: 05 назв.

UDC 681.3.06

The method of designing and verifying functions of trusted computing base for protection from unauthorized access /A.V. Lyenshyn // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 328—332.

A comprehensive approach to the design and verification of trusted computing base for protection from unauthorized access is offered. An approach to create and use templates for algorithms of implementing security services in a formal Parondzhanov notation is analyzed. An example of using the method for developing the algorithm of realizing the "failure recovery" service created with the proposed templates is given.

Keywords: protection from unauthorized access, technical information protection regulatory document 2.5-004-99, system analysis, dragon schemes, Parondzhanov notation.

Tab.: 01. Fig.: 02. Ref.: 05 items.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНДАРТИЗОВАНИХ ВЕРСІЙ КРИПТОАЛГОРИТМУ ECIES

І.Д. ГОРБЕНКО, М.І. ХАРЛАМБ

Криптографія на еліптичних кривих (КЕК) може бути використана як інструмент для шифрування даних, створення цифрових підписів або в ході виконання обміну ключовими даними. Інтегрований механізм шифрування (ECIES) є відомою схемою, заснованою на КЕК, тому він був включений в кілька криптографічних стандартів. У даній роботі надається огляд і порівняння версій ECIES, включених у документи ANSI, IEEE, ISO / IEC, і SECG, виділяються основні відмінності між ними та можливості використання схеми для різних систем.

Ключові слова: протокол шифрування, криптографія з відкритим ключем, ECIES.

ВСТУП

З розвитком криптографії з відкритим ключем Діффі і Геллманом у 1976 році, було запропоновано декілька криптосистем. У будь-якій криптосистемі головними особливостями є ступінь захищеності та ефективність, проблема забезпечення яких завжди належить до математичної бази, на якій її засновано. На сьогодні обчислювано неможливими вважаються: задача дискретного логарифмування, задача факторизації цілих чисел та задача дискретного логарифмування на еліптичних кривих.

У 1985 році Мілер та Кобільц незалежно один від одного запропонували криптосистему, що заснована на використанні еліптичних кривих у скінченних полях, стійкість яких заснована на дискретному логарифмуванні на еліптичних кривих. У порівнянні з іншими криптосистемами (такими як RSA), криптографічні методи, засновані на еліптичних кривих, використовують ключ значно меншої довжини. Причина цього пов'язана із високою стійкістю поданих систем, що, як вважає більшість спеціалістів, пов'язана із значною складністю розв'язання математичних рівнянь, ніж це можна розглядати при дискретному логарифмуванні чи факторизації цілих чисел.

На сьогодні з усіх відомих криптоалгоритмів, заснованих на еліптичних кривих, можна виділити інтегрований механізм шифрування на еліптичних кривих¹. У даній роботі ми надаємо детальний аналіз та порівняння існуючих версій цього механізму, використовуючи офіційні документи та стандарти [1–3] та виділяючи головні відмінності в них, що можуть бути повністю сумісними в ході використання різних версій.

Робота побудована так, що в першій частині наведені положення щодо функціонального дизайну механізму, розділ 2 порівнює його різні версії за функціональним складом, розділ 3 демонструє стандартний набір функцій у кожній версії стандарту, в четвертому розділі підбиваються підсумки роботи та робляться висновки з проведених аналізів та отриманих результатів.

¹ Elliptic Curve Integrated Encryption Scheme (ECIES)

1. ІНТЕГРОВАННИЙ МЕХАНІЗМ ШИФРУВАННЯ НА ЕЛІПТИЧНИХ КРИВИХ

У 1997 році Міхір Белар та Філіп Рогавей представили світу доповнений механізм шифрування на дискретному логарифмі², який згодом був довершений ними та Мікаелем Абдалою. Тоді в перший раз алгоритм був названий доповненим механізмом шифрування Діффі-Геллмана, а пізніше, у 1998 році, інтегрованим алгоритмом шифрування Діффі-Геллмана, з метою уникання колізій у назві з доповненим алгоритмом шифрування³.

Механізм інтегрованого шифрування є довершеною схемою шифрування Ель-Гамала, використовуючи інтегровану криптографію еліптичних кривих, що включає операції з відкритими ключами, схеми шифрування, MAC-коди та геш-значення. Завдяки інтеграції перелічених функцій, цей механізм є стійким проти атак на шифротекст без необхідності збільшення кількості заснованих операцій чи довжини ключа.

На схемі 1 наведено модель роботи алгоритму з [9], де M – це вхідне повідомлення, g – генератор мультиплікативної групи G , g_u , g_v – відкриті ключі отримувача та відправника, u та v – секретні ключі отримувача та відправник, ε – симетричний алгоритм шифрування, τ – функція генерації MAC-кодів, H – геш-функція. Даний механізм був дороблений ANSI⁴ та з деякими модифікаціями включений до стандарту ANSI X9.63 у 2001 році. Незалежно від цього IEEE у 2000 році затвердила стандарт IEEE 1363. Коли у 2004 році ANSI X9.63 було надано широкому розголосу, IEEE розглянув обидві версії та запропонував новий стандарт 1363a. Всі ці версії об'єдналися під однією назвою ECIES (Elliptic Curve Integrated Encryption Scheme), але їх не можна назвати ідентичними.

Протягом останніх років ще одна група вчених з ISO/IEC об'єдналася для прийняття стан-

² Discrete Logarithm Augmented Encryption Scheme (DLAES)

³ Advanced Encryption Standard (AES)

⁴ ANSI – American National Standards Institute

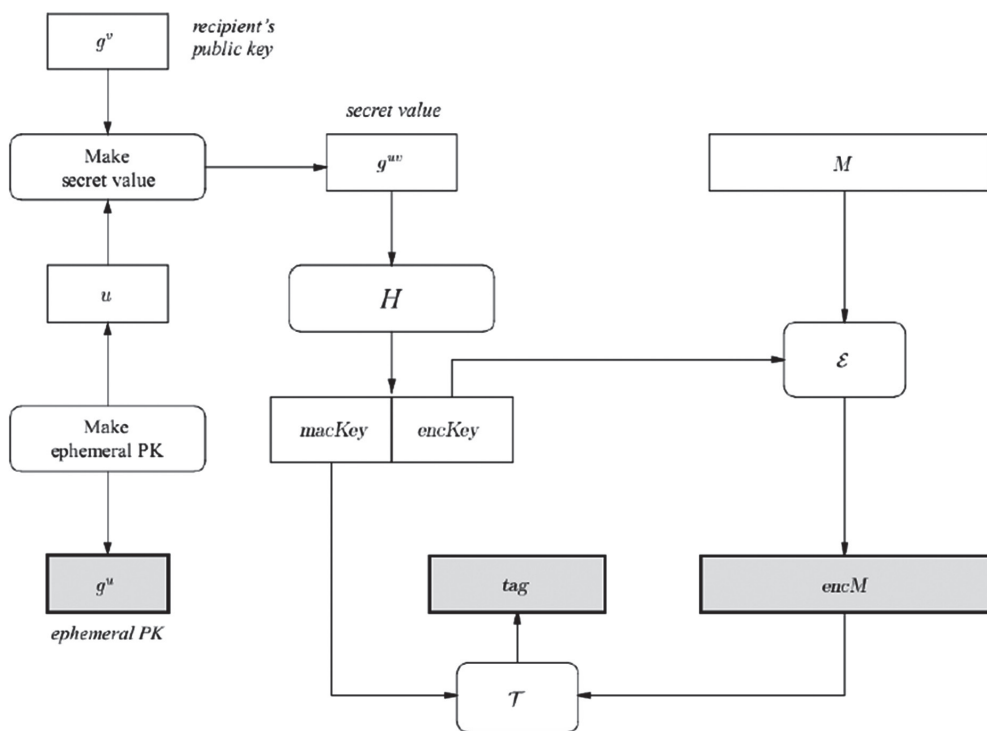


Схема 1. DHIES функціональна схема

дарту сімейства 18033. За основу вони взяли усі існуючі на той момент версії ECIES та базові дослідження стійкості алгоритму. В результаті з'явилася ще одна версія стандарту, що була додана до ISO/IEC 18033-2 у 2006 році.

Таким чином, головним документом стандарту прийнято вважати опис алгоритму ECIES, що був прийнятий на консорціумі групи із стандартизації криптографічних продуктів у 2000 році, та дороблений у 2009 році.

2. БАЗОВІ КОНЦЕПЦІЇ МЕХАНІЗМУ

Як визначає назва алгоритму, ECIES інтегрує схему шифрування, використовуючи такі функції:

- Функція генерації ключів (ФГК). Використовується для вироблення спільного секретного ключа між двома абонентами.
- Функція вироблення ключів (ФВК). Механізм застосовується для вироблення ключів з вихідного матеріалу та параметрів.
- Геш-функція (ГФ). Функція, що дозволяє генерувати геш-значення для будь-якого повідомлення.
- Алгоритм шифрування (АШ). Симетричний алгоритм шифрування.
- Код автентифікації повідомлення (КАП). Необхідний для того, щоб ідентифікувати повідомлення.

Після порівняння версій схеми шифрування ANSI, IEEE, ISO/IEC та SECG можна виділити дві групи різновидів:

- Функціональні: деталі реалізації, опції, подання у двійковому вигляді тощо.
- Вибір між існуючими алгоритмами: алгоритми шифрування, геш-функції тощо [1].

3. ПОРІВНЯННЯ ФУНКЦІОНАЛЬНОСТІ ВЕРСІЙ

У цьому розділі ми проаналізуємо версії механізму попарно та знайдемо відмінності між існуючими версіями.

DHIES та ANSI X9.63

• Наведемо головні відмінності між оригінальною версією механізму DHIES та його імплементацією ANSI X9.63:

• DHIES не дозволяє використання довільних параметрів у функції виготовлення ключів та у функції генерування коду повідомлення, в той час як ANSI X9.63 припускає такий варіант.

• DHIES використовує функцію шифрування для генерації коду повідомлення та для формування геш-значення. ANSI X9.63 використовує конструкцію, де дані проходять декілька раундів.

• DHIES інтерпретує ліві біти на виході як значення функції генерації ключів, а праві як MAC-код повідомлення. ANSI X9.63 виконує навпаки.

• DHIES дозволяє використовувати як алгоритми симетричного шифрування поточкові або блокові шифри, крім того залишається можливість використовувати альтернативні алгоритми. X9.63 дозволяє використання тільки функції XOR.

ANSI X9.63 та IEEE 1363a

У цьому розділі порівнюємо стандарти ANSI X9.63 та IEEE 1363a

• ANSI X9.63 дозволяє як функція вироблення спільного секрету лише схема Діффі-Геллмана, IEEE 1363a підтримує її використання, але і дозволяє застосовувати альтернативний варіант.

- ANSI X9.63 дозволяє використовувати довільні параметри для функції вироблення ключів, але не вимагає чітких вимог до цих параметрів. IEEE 1363a використовує двійкове уявлення відкритого ключа відправника як вхідний параметр.

- ANSI X9.63 використовує першу координату, генеровану функцією вироблення спільного секрету, коли IEEE 1363a використовує елемент у цілому.

- ANSI X9.63 завжди перетворює ліву частину бітів функції вироблення ключів як ключ шифрування та праву частину, як код автентифікації повідомлення. IEEE 1363a інтерпретує вихідний потік як $kMAC || kENC$, коли використовується поточний шифр та навпаки, коли використовується блоковий [2–4].

IEEE 1363a та ISO/IEC 18033-2

У цьому розділі порівнюємо стандарти ISO/IEC 18033-2 та IEEE 1363a

- IEEE 1363a дозволяє використовувати довільні параметри у функції генерації ключів, але ISO/IEC 18033-2 не дозволяє це робити.

- IEEE 1363a дозволяє обробляти повідомлення як в бітовому, так і в байтовому уявленні. ISO/IEC 18033-2 підтримує роботу тільки з байтовими рядками.

- IEEE 1363a вимагає завжди використовувати однаковий набір параметрів для даного відкритого ключа. ISO/IEC 18033-2 дозволяє змінювати параметри і функції залежно від ключа.

- IEEE 1363a вимагає мінімальну довжину ключа 160 біт. ISO/IEC 18033-2 не вимагає мінімальної довжини ключа.

Ці відмінності прибрали з останніх версій стандартів для того, щоб забезпечити вищий рівень сумісності між схемами [1–2].

ISO/IEC 18033-2 та SECG SEC 1

У цьому розділі порівнюємо стандарти ISO/IEC 18033-2 та SECG SEC 1.

- ISO/IEC 18033-2 не вимагає вхідних параметрів до функції вироблення ключів, в той час як SEC 1 потребує цю інформацію.

- SEC 1 не вимагає включення відкритого ключа відправника до функції виготовлення ключів. Тут відкритий ключ розглядається як вхідний параметр.

- ISO/IEC 18033-2 не потребує мінімальної довжини ключа.

4. ФУНКЦІОНАЛЬНІ СКЛАДОВІ МЕХАНІЗМУ

В цій частині розглянемо функції та додатки, що використовуються в механізмі для створення проміжних параметрів та формування шифротексту: функція генерування ключів, функція вироблення MAC-коду повідомлення, алгоритм шифрування, геш-функція. Основні положення наведені у вигляді табл. 1.

Пояснення до табл. 1 :

- DH – механізм обміну спільним секретом Діффі-Геллмана.

- X9.63-KDF – описано в [10], KDF1 та KDF2 розглядаються в [13], функція NIST-800-56 KDF конкатенації з [18].

- SHA-1, SHA-2(256, 384, 512), RIPEMD, WHIRPOOL – геш-алгоритми формування значень.

- TDES – Triple DES алгоритм, що виконує шифрування. Разом з ним використовується стандарт AES – (28, 192, 256), MISTY1, CAST-128.

- DEA, HMAC-SHA (..), CMAC-AES – функції для формування MAC-коду повідомлення.

ВИСНОВКИ

Після детального аналізу відмінностей між версіями механізму ECIES стає явним той факт, що в одному програмному компоненті неможливо поєднати використання усіх стандартів.

Крім того, реалізації можуть зіткнутися з ще однією важливою проблемою, яку можна сформулювати як обмеження у функціях, доступних для розробника інтерфейсу програмування ці-

Таблиця 1

Функції та алгоритми стандартів сімейства ECIES

	X9.63	1363a	18033-2	SEC 1
KA	DH	DH DHC	DH DHC	DH DHC
KDF	X9.63-KDF	X9.63-KDF	KDF1 KDF2	X9.63-KDF NIST-800-56
HASH	SHA-1	SHA-1 SHA-2 RIPEMD	SHA-1 SHA-2 RIPEMD WHIRLPOOL	SHA-1 SHA-2*
ENC	XOR	TDES AES	TDES AES MISTY1 CAST-128	XOR AES
MAC	DEA ANSI X9.71	MAC1	H-SHA-1 H-SHA-2 H-RIPEMD	H-SHA-1 H-SHA-2* CMAC-AES

льового продукту. Прямим наслідком є те, що під час застосовування ECIES, першим кроком має бути оцінка можливостей кінцевої платформи використання та аналіз призначення з тієї точки зору, щоб вирішити яка версія ECIES є адекватною для конкретного використання.

Нові версії (наприклад, ISO / IEC 18033-2 iSEC 1) не можуть бути повністю сумісні з успадкованими пристроями, але вони забезпечують доступ до новіших стійких функцій (наприклад, SHA-2, AES і т.д.), тому вони повинні рекомендовано використовувати одну з цих версій.

Література

- [1] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. 22, pp. 644–654, 1976.
- [2] Електронний ресурс: <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf><https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
- [3] T. Mather, S. Kumaraswamy, S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'ReillyMedia, 2009. — 334 с.
- [4] Електронний ресурс: http://www.cryptopp.com/wiki/Elliptic_Curve_Integrated_Encryption_Scheme
- [5] BSI TR 03111, Elliptic Curve Cryptography, Bundesamt für Sicherheit in der Informationstechnik, 2009, <http://www.bsi.de/literat/tr/tr03111/BSI-TR-03111.pdf>.
- [6] J. H. Silverman, The Arithmetic of Elliptic Curves, ser. Graduate texts in Mathematics. New York, NY, USA: Springer-Verlag, 1986, vol. 106.
- [7] M. Bellare and P. Rogaway, "Minimizing the use of random oracles in authenticated encryption schemes," Lecture Notes in Comput. Sci., vol. 1334, pp. 1–16, 1997.
- [8] M. Abdalla, M. Bellare, and P. Rogaway, DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem, contribution to IEEE P1363a, 1998, <http://grouper.ieee.org/groups/1363/P1363a/contributions/dhaes.pdf>.

Надійшла до редколегії 21.06.2014



Харламб Марія Ігорівна, студентка 5-го курсу кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: програмування, криптографічні методи захисту інформації, хмарні технології.

УДК 004.75:004:0.5

Сравнительный анализ стандартизированных версий криптоалгоритма ECIES / И.Д. Горбенко, М.И. Харламб // Прикладная радиоэлектроника: науч.-техн. журнал. — 2014. — Том 13. — № 1. — С. 333–336.

Криптография на эллиптических кривых (КЭК) может быть использована как инструмент для шифрования данных, создания цифровых подписей или при выполнении обмена ключевыми данными. Интегрированный механизм шифрования (ECIES) является известной схемой, основанной на КЭК, поэтому он был включен в несколько криптографических стандартов. В данной работе предоставляется обзор и сравнение версий ECIES, включенных в документы ANSI, IEEE, ISO / IEC, и SECG, выделяются основные различия между ними и возможности использования схемы для различных систем.

Ключевые слова: протокол шифрования, криптография с открытым ключом, ECIES.

Табл.: 01. Ил.: 01. Библиогр.: 08 назв.

UDC 004.75:004:0.5

Comparative analysis of standardized versions of cryptographic algorithm ECIES / I.D. Gorbenko, M.I. Kharlam // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 1. — P. 333–336.

Elliptic Curve Cryptography (ECC) can be used as a tool for data encryption, creation of digital signatures or performing of key data exchange. Integrated encryption mechanism (ECIES) is a well-known scheme based on the ECC, so it was included in several cryptographic standards. This paper provides an overview and comparison of ECIES versions included in ANSI, IEEE, ISO / IEC, and SECG documents, and highlights the main differences between them and the possibility of using the scheme for different systems.

Keywords: encryption protocol, public key cryptography, ECIES.

Tab.: 01. Fig.: 01. Ref.: 08 items.

КРИПТОГРАФИЯ НОВОГО ПОКОЛЕНИЯ: ИНТЕГРАЛЬНЫЕ УРАВНЕНИЯ КАК АЛЬТЕРНАТИВА АЛГЕБРАИЧЕСКОЙ МЕТОДОЛОГИИ*

Г.К. БРОНШПАК, И.А. ГРОМЫКО, С.И. ДОЦЕНКО, Е.Л. ПЕРЧИК

Показаны преимущества использования в криптографии положений математического анализа, обусловленные свойством функций непрерывного аргумента. В качестве них могут выступать как предварительно представленные рядами графики, таблицы, видеоизображения, так и буквы, числа, символы, в соответствие которым поставлены, например, синусы разной амплитуды. Шифрование производится путем интегрирования функций, дешифрование — путем решения интегральных уравнений. Приведены примеры реализации данных процедур в аналитическом виде. Многообразие вариантов таких преобразований, включая их применение в комбинациях, ставит перед криптоанализом практически непреодолимые проблемы. Рассмотрена возможность использования для криптографической защиты известных решений задач математической физики. Проанализирована сущность высокой эффективности шифрования, базирующаяся на зависимости функций от неограниченного числа информативных признаков.

Ключевые слова: криптография, непрерывный анализ, интегрирование, интегральные уравнения, формулы обращения.

ВВЕДЕНИЕ

В одном из источников по криптографии встретила трактовка: $A\psi = f$ — шифрование; $\psi = A^{-1}f$ — дешифрование. Возник вопрос: может ли оператор A быть интегральным? Подразумевается следующее:

- шифрование функции $\psi(x)$ путем воздействия интегрального оператора A , как $f(x) = (A\psi)(x)$;

- дешифрование функции $f(x)$, восстановление $\psi(x)$ путем решения интегрального уравнения $(A\psi)(x) = f(x)$, т. е. $\psi(x) = (A^{-1}f)(x)$;

- соответственно, функция ψ , несущая информацию, должна быть интегрируемой, далее полагаем, что она является однозначной и кусочно-непрерывной.

Однако уловить хотя бы признаки обозначенного подхода в весьма обширной литературе по криптологии не удалось. При этом данная область знаний, будучи очень важной, для практических приложений, разрабатывается весьма интенсивно; накоплены колоссальные объемы материалов по результатам проведенных исследований, которые характеризуются как глубиной логических построений, так и, можно сказать, изощренностью алгоритмических средств реализации. Зримо ощущим громадный труд специалистов за продолжительный период времени. Наряду с чем подчеркивается — основу, как криптографии, так и криптологии, в целом, составляет аппарат дискретной математики, — это преимущественно алгебраическая наука, что в полной мере подтверждают многочисленные публикации. Но математику обычно подразделяют на арифметику, алгебру и анализ (функции непрерывного аргумента, дифференцирование,

интегрирование и т. д.), в криптологии, что следует подчеркнуть, отсутствующий.

Поэтому возникают вопросы:

- нельзя ли отнести его (анализа) отсутствие на счет неких факторов историко-субъективистского свойства (по типу незыблемости идей основоположников), инициировавших высокую плотность исследований в рамках именно «алгебраической» криптографии (АК);

- не тесны ли упомянутые рамки для разрешения фундаментальных проблем криптографии с позиций их всеобъемлюще объективной постановки, а также последующего разрешения путем проведения аналитических исследований;

- иначе говоря, какой конструктивизм способен придать аппарат анализа, в первую очередь, преобразования с оператором A (см. выше), криптографии, которую назовем «интегральной» (ИК)?

Цель статьи состоит в том, чтобы на методологическом уровне продемонстрировать высокий потенциал ИК, с точки зрения защиты информации, поскольку для этого возникают качественно новые возможности, не имеющие аналогов в АК. В первую очередь, имеется в виду зависимость функции от непрерывно изменяющегося аргумента. По существу, ниже характеризуется направление глобального исследования проблемы криптографической защиты, с позиций ее практической реализации, которое является, казалось бы, совершенно очевидным, однако в силу непонятных нам причин осталось вне поля зрения специалистов.

В самом деле, — это необъяснимый парадокс, а именно: существует своего рода кладь алгоритмических средств математического анализа, из которого практически без усилий можно черпать исключительно эффективные, по нашему мнению, варианты организации криптографической защиты. В житейской интерпретации ситуацию можно пояснить и так. Если нужно вырыть

* Статья публикуется как проблемная и редакция надеется, что она более детально будет рассмотрена специалистами.

котлован, то в принципе для этого занятия подходит множество предметов, включая атрибутику бытового обихода. Однако, игнорирование в процессе принятия решений преимуществ экскаватора (подразумеваем непрерывный анализ) представляет собой, очевидно, парадокс, который в полной мере аналогичен рассматриваемой ситуации.

1. НЕТРИВИАЛЬНАЯ СОПРЯЖЕННОСТЬ АК И ИК

Известен аналитический метод шифрования АК [1, с. 20–22]:

$$\sum_{j=1}^n a_{ij} \psi_j = f_i, i = 1, \dots, n, \quad (1)$$

где $\psi = \{\psi_j\}$ — вектор целых чисел, отвечающих номерам букв некоторого алфавита; $\{a_{ij}\}$ — целочисленная квадратная матрица того же порядка n . К достоинствам такого подхода относят возможность восстановления вектора ψ путем целочисленных преобразований, что исключает погрешность счета, а значит, и неустойчивость используемого алгоритма. Развитию теории данного класса задач посвящена книга [2], прямо не касающаяся криптографии.

Однако не следует выбирать n в (1) достаточно большим, поскольку возможны проблемы, связанные с переполнением машинной памяти, или же появлением машинного нуля [3, п. 14.3]. Наряду с чем, вычисление элементов ψ_i из системы (1), которое фактически производится по правилу Крамера, если, например, $n = 20$, даже на современном этапе, развития техники, требует совершенно нереалистичных затрат машинного времени, фигурирует порядок 10^8 лет [4, с. 43–44].

В свете сказанного, $n \rightarrow \infty$ кажется абсурдным. Однако, как отметил Р. Кук: «в то время как теория конечных матриц является частью алгебры, теория бесконечных матриц составляет раздел анализа» [5, с. 13] (заметим, говорят также классический, или непрерывный анализ, подчеркивая характер зависимости от аргумента). Действительно, пусть ψ_j — ординаты бесконечной последовательности чисел (хотя бы и целых), расставленные с шагом Δx вдоль оси абсцисс. Если формально обозначить

$$a_{ij} = k_{ij} \Delta x, i, j = 1, \dots, n, \quad (2)$$

то соотношения (1) приобретают вид

$$\sum_{j=1}^n k_{ij} \psi_j \Delta x = f_i, i = 1, 2, \dots, n; \quad (3)$$

однако, вследствие (2) элементы матрицы

$$\{k_{ij}\}, i, j = 1, 2, \dots, n, \quad (4)$$

в общем случае, не представляют собой целые числа, а значит, достоинства аналитического метода АК полностью утрачиваются.

Но, на самом деле, в смысле разрешения глобальной проблемы криптографии мы получаем

колоссальные преимущества. Действительно, если представить компоненты (3) в эквивалентном виде, несколько изменив обозначения:

$$k_{ij} = k(x_i, \xi_j); \psi_j = \psi(\xi_j); f_i = f(\xi_i), \quad (5)$$

где $x_i = i \Delta x$; $\xi_j = j \Delta \xi$, $\Delta x = \Delta \xi$, координаты вектора $f = \{f_i\}$ определяем как

$$\sum_{j=1}^n k(x_i, \xi_j) \psi(\xi_j) \Delta x = f(x_i), i = 1, 2, \dots, n \quad (6)$$

(суммирование производится по точкам ξ_j ; значения в точках x_i данной процедуры играют роль параметров).

Рассматривая, для определенности, отрезок $0 \leq x \leq 1$, посредством перехода в (6) к пределу $n \rightarrow \infty$, соответственно $\Delta x \rightarrow 0$, на основании классического определения интеграла получаем

$$(A\psi)(x) = \int_0^1 k(x, \xi) \psi(\xi) d\xi = f(x), x \in [0, 1] \quad (7)$$

(совокупности значений (5) превращаются в функции непрерывного аргумента; $\Delta \xi$ обращается в дифференциал $d\xi$). Относительно функции $\psi(x)$ — это интегральное уравнение Фредгольма первого рода, с ядром $k(x, \xi)$. Мы вернемся к его рассмотрению ниже (п. 5).

Очевидно, $x_i = x$ и $\xi_j = \xi$, когда $n \rightarrow \infty$. Таким образом, вместо вектора (1), располагающегося на интервале бесконечной длины, «нужную» ∞ мы организовали посредством разбиения отрезка $0 \leq x \leq 1$ на бесконечно малые части:

$$\frac{1}{\Delta x} = \infty, \Delta x \rightarrow 0, \quad (8)$$

иначе говоря, предельный переход от (6) к (7) осуществляется как

$$\lim_{n \rightarrow \infty} \sum_{j=1}^n k(x_i, \xi_j) \psi_j(\xi_j) \Delta \xi = \int_0^1 k(x, \xi) \psi(\xi) d\xi$$

и, вместе с тем, здесь присутствует тонкий момент. Действительно, если значения k_{ij} элементов матрицы (4) — конечны, то в условиях (8) элементы матрицы $\{a_{ij}\}$, согласно (2), являются бесконечно малыми. Возникает вопрос в том плане, что умножение «бесконечно малой» матрицы на вектор (1) кажется непривычным, и нет ли для этого специальной теории?

Ответ простой — подобного рода теория в данном случае не актуальна, поскольку без использования приведенных преобразований, а соответственно и аналитического метода АК, «шифровку» $f(x)$, или же уравнение (7), можно получить с помощью сугубо формального приема, а именно путем воздействия оператора

$$A. = \int_0^1 k(x, \xi). d\xi, \quad (9)$$

где ядро $k(x, \xi)$ выбирается произвольно, на функцию $\psi(x)$. Иначе говоря, в рамках исключительно ИК. В этой связи обратим внимание на ключевой, как представляется, момент настоящего изложения.

Если АК, согласно (1), имеет $n \times n$ шифрующих, скажем так, параметров a_{ij} (в примере [1] $n=3$), то у ядра $k(x, \xi)$ в (9), их бесконечное множество (точки двумерной функции от непрерывных аргументов). Как соотносить друг с другом по эффективности шифрования ∞ и $n^2=9$? Вполне очевидный ответ на этот вопрос убедительно поясняет колоссальные преимущества ИК, о которых, декларативно, упоминалось выше. Заметим также, что вследствие сказанного в отношении (9) осцилляции k_{ij} из (2), обусловленные выбором элементов a_{ij} , становятся несущественными. Мы просто исключаем процедуру упомянутого выбора, она становится ненужной, поскольку ИК ни как не базируется на АК в конструктивном смысле и, тем не менее, искусственно «погрузив» АК в непрерывный анализ, можно судить о взаимосвязанности методов.

2. ПРЕДСТАВЛЕНИЕ ИНФОРМАЦИИ И ТАКТИКА ЕЕ ЗАЩИТЫ

Итак, функция $\psi(x)$ предполагается однозначной и кусочно-непрерывной. Она может представлять:

- аналитические зависимости переменной x разнообразного содержания;
- графики, в частности, акустических амплитуд речевых сообщений, результатов геологических зондирований, тех же кардиограмм;
- фрагменты видеоизображений, сопряжение которых снимает ограничение на однозначность функции $\psi(x)$;
- таблицы чисел, для которых априори предусмотрен способ аппроксимации (так, что после преобразований можно восстановить исходную дискретность), по типу гистограмм;
- буквы, цифры, пробелы текстов, математические символы и другие обозначения, которые трактуются как непрерывные функции, в частности:

$$\psi_s(x) = \alpha_s; \psi(x) = \beta_s \sin \omega_s x, x \in [0, 1], s = 1, 2, \dots, (10)$$

где $\alpha_s, \beta_s, \omega_s$ — константы; s — номер обозначения в соответствующем алфавите.

Назовем функции: $\psi(x)$ — сообщение; $f(x)$ — зашифрованное сообщение, шифрограмма, или же — шифровка. Фигуранты рассматриваемого процесса и «правила игры»:

- отправитель шифровки $f(x)$, он же автор сообщения $\psi(x)$;
- адресат (коллега, партнер отправителя и т. п.) — лицо, которому предназначено сообщение $\psi(x)$, после дешифрования $f(x)$;
- оппонент — лицо, преследующее целью дешифровать $f(x)$, средствами криптоанализа, для ознакомления с сообщением $\psi(x)$;
- конечно же, предполагается, что оппонент не имеет информации об операторах A, A^{-1} , кстати, как и адресат (см. ниже);
- шифровка $f(x)$ размещается на сайте, практически свободного доступа, становясь из-

вестной как адресату, так и оппоненту (очевидно, они могут быть в неединственном количестве);

- по существу $f(x)$ представляет собой именно шифрограмму — кривая на графике, очертание которой поддается подробной детализации (можно назвать ее и видеоизображением);

- предварительно в компьютер адресата отправителем заложен блок программ, позволяющих в автоматическом режиме восстанавливать сообщения $\psi(x)$ по шифровкам $f(x)$;

- упомянутый блок, прямой доступ к которому адресата жестко заблокирован, охватывает весьма большое количество M вариантов программных реализаций и обновляется через достаточно продолжительные периоды времени;

- напротив, номер режима работы $m = 1, 2, \dots, M$ может быть изменен отправителем в произвольном порядке и сообщается адресату практически открыто, в частности, по телефону.

Что же представляют собой m -варианты программ? Это синхронизированные с шифрованием обратные процедуры восстановления $\psi(x)$ по данной шифровке $f(x)$. Причем факторами надежности, как шифрования, так и соответственно создания практически непреодолимых препятствий для криптоаналитики оппонентов выступают следующие обстоятельства (они могут реализовываться в комплексе, что следует подчеркнуть):

- деформация (попросту говоря, искажение) сообщения $\psi(x)$ под воздействием интегрального оператора A (см. конкретные примеры ниже, пп. 3 — 6);

- использование повторных $A^n, n \geq 2$, а также комбинированных $A_1 A_2 \dots$ воздействий интегральных операторов различных типов и вида;

- перестановки частей кривых $f(x)$ на графике, а также добавление к ним «ложных» участков (можно предположить, что эффективность таких действий с функциями будет гораздо выше по сравнению с АК, где они применяются для таблиц чисел).

В свете сказанного возникает вопрос о том — можно ли получить количественную оценку эффективности шифрования? Как представляется, здесь трудно предложить что-либо за исключением показателя, характеризующего средний уровень «непохожести», скажем так, нормированных функций $\psi(x)$ и $f(x)$ вида:

$$\mu = \int_0^1 \left[\frac{\psi(x)}{\sqrt{\|\psi\|}} - \frac{f(x)}{\sqrt{\|f\|}} \right]^2 dx, \quad (11)$$

$$\|\psi\| = \int_0^1 \psi^2(x) dx; \|f\| = \int_0^1 f^2(x) dx,$$

или же учесть, в дополнение, большую важность отдельных локализаций по аргументу x с помощью весовых множителей.

3. ПРИМЕРЫ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ В ЗАМКНУТОМ ВИДЕ

Интеграл

$$(A\psi)(x) = \int_0^x [a(x-\xi) + c] \psi(\xi) d\xi = f(x), \quad (12)$$

где a, c — произвольные константы, имеет формулу обращения [6, с. 15]:

$$\begin{aligned} \psi(x) &= (A^{-1}f)(x) = \\ &= \frac{1}{c} \frac{d}{dx} \left[\exp\left(-\frac{a}{c}x\right) \int_0^x \exp\left(\frac{a}{c}\xi\right) \frac{d}{d\xi} f(\xi) d\xi \right]; \end{aligned} \quad (13)$$

иначе говоря, (13) представляет собой решение в замкнутом виде интегрального уравнения Вольтерра первого рода (12). Обратимся к первой из функций (10), полагая $\alpha_s \equiv 1$, а значит

$$\psi(x) = 1, \quad (14)$$

и целесообразно воспроизвести все преобразования на основе (12), (13) с тем, чтобы нас было бы легко проверить.

Интегрируя, согласно (12), получаем

$$f(x) = 0,5ax^2 + cx, \quad (15)$$

соответственно в (13)

$$\frac{d}{d\xi} f(\xi) = a\xi + c$$

и далее:

$$\int_0^x \exp\left(\frac{a}{c}\xi\right) \frac{d}{d\xi} f(\xi) d\xi = cx \exp\left(\frac{a}{c}x\right);$$

умножение этого выражения на $\exp(-ax/c)$ и дифференцирование $c^{-1}d/dx$ восстанавливают (14).

По такой схеме может действовать программа дешифрования с использованием табличных операций интегрирования. Однако упростим задачу, предполагая, что сообщение состоит из последовательности чисел α_s . Зная это, программа определит α_s путем деления значений ординат на шифрограмме и графике (15) при том же аргументе x , поскольку соответствующие им кривые подобны. То есть, оказалось возможным обойтись без формулы обращения (13). И главное, кто скажет, по виду шифровки (15), что она похожа на сообщение (14) в условиях, когда константы a, c варьируются, образно выражаясь, во времени и пространстве? Иначе говоря, как между сообщениями, так и внутри них.

Пусть теперь в (10), а соответственно и (12), функция

$$\psi(x) = \sin \omega x; \quad (16)$$

тогда шифровка посредством интегрирования приобретает вид

$$\begin{aligned} f(x) &= \int_0^x (ax - a\xi + c) \sin \omega \xi d\xi = \\ &= \frac{1}{\omega} (ax + c) - \frac{c}{\omega} \cos \omega x - \frac{a}{\omega^2} \sin \omega x, \end{aligned} \quad (17)$$

соответственно в (2)

$$\frac{d}{d\xi} f(\xi) = \frac{a}{\omega} + c \sin \omega \xi - \frac{a}{\omega} \cos \omega \xi$$

и далее:

$$\begin{aligned} \int_0^x \exp\left(\frac{a}{c}\xi\right) \left(\frac{a}{\omega} + c \sin \omega \xi - \frac{a}{\omega} \cos \omega \xi \right) d\xi &= \frac{c}{\omega} e^{\frac{a}{c}x} + \\ &+ \frac{ce^{\frac{a}{c}x}}{\left(\frac{a}{c}\right)^2 + \omega^2} \left(\frac{a}{c} \sin \omega x - \omega \cos \omega x \right) - \\ &- \frac{\frac{a}{\omega} e^{\frac{a}{c}x}}{\left(\frac{a}{c}\right)^2 + \omega^2} \left(\frac{a}{c} \cos \omega x + \omega \sin \omega x \right); \end{aligned}$$

умножение этого выражения на $\exp(-ax/c)$ и дифференцирование $c^{-1}d/dx$ приводят к (16). То есть, исходная информация восстановлена.

Обратим внимание на следующие моменты:

— шифровка (17), аналогично (15), совсем не напоминает сообщение (16) и значение μ в (11) видится достаточно внушительным;

— представляет интерес построение, в аналитическом виде, рекуррентных соотношений для степеней A^n , $(A^n)^{-1}$, где A — интегральный оператор (12);

— если функция $\psi(x)$ представлена графически, принципиально отличительных особенностей в процессе преобразований, сравнительно с (16), не возникает, поскольку можно воспользоваться разложением в ряд Фурье:

$$\psi(x) = \sum_n a_n \sin \omega_n x.$$

Известен метод шифрования, посредством умножения большого количества целых чисел (односторонние преобразования). Периодически сообщается о том, что с использованием столько-то тысяч компьютеров, продолжительность работы которых измеряется в месяцах, удалось разложить на множители результат умножения, а значит произвести дешифрование сложного сообщения. В общем, здесь своеобразный спорт и реклама. Возникает любопытный вопрос: способен ли существующий криптоанализ по графикам функций (15) и (17) определить, что они представляют собой простейшие, заметим, шифровки соответственно 1 и $\sin \omega x$?

У нас большие сомнения, хотя бы потому, что криптоанализ не имеет опыта обращения с «непрерывностью».

4. ИНТЕГРАЛЫ И АНАЛИТИЧЕСКИЕ ФОРМУЛЫ ОБРАЩЕНИЯ

Рассмотрим ряд интегральных уравнений, которые представляются весьма полезными для решения задач криптографии. Уравнения, за исключением одного, взяты из справочника [6], где они дифференцированы в разрезе:

- первого и второго рода (соответственно, функция $\psi(x)$ находится только под интегралом, или также и в явном виде, т. е. вне интеграла);
- пределы интегрирования постоянные, или же одним из них является x .

Пример 1

$$(A\psi)(x) = \int_{\rho}^x (ax + b\xi + c)\psi(\xi)d\xi = f(x), \quad (18)$$

где a, b, c и ρ — произвольные константы. Заметим, что уравнение (12) представляет частный случай (18), когда $b = -a$, $\rho = 0$. Таким образом, в (18) появились две дополнительные константы b и ρ , объективно затрудняющие криптоанализу оппонента.

Формулы обращения интеграла (18) для случаев $b \neq -a$ и $b = -a$ имеют вид соответственно:

$$\psi(x) = d_x \left\{ \left[(a+b)x + c \right]^{-\frac{a}{a+b}} \int_{\alpha}^x \left[(a+b)\xi + c \right]^{\frac{b}{a+b}} d_{\xi} f(\xi) d\xi \right\};$$

$$\psi(x) = \frac{1}{c} d_x \left[\exp\left(-\frac{a}{c}x\right) \int_{\alpha}^x \exp\left(\frac{a}{c}\xi\right) d_{\xi} f(\xi) d\xi \right],$$

где $d_x = d/dx$. Однако, предположим, что конкурент догадается продифференцировать функцию $f(x)$ из (18). Тогда он получает интегральное уравнение Вольтерра второго рода:

$$\psi(x) + \frac{a}{c + (a+b)x} \int_{\rho}^x \psi(\xi) d\xi = \frac{d_x f(x)}{c + (a+b)x} \quad (19)$$

с присутствием искомой функции $\psi(x)$ в явном виде.

Если речь идет об идентификации аномалии качественного характера на графике, свидетельствующей в пользу локализации месторождения, или же волнений финансового рынка, оппонент может добиться преимущества. Особенности, присущие функции $\psi(x)$, будут выделяться на фоне сглаженной интегрированием компоненты. С другой стороны, процедуры численного дифференцирования весьма не точны а, разлагая предварительно функцию $f(x)$ в некоторый ряд, оппонент способен нивелировать имеющиеся у нее особенности.

Пример 2

$$(A\psi)(x) = \int_0^x \frac{\psi(\xi)d\xi}{x+\xi} = f(x) = \sum_{n=0}^N a_n x^n,$$

где a_n — постоянные коэффициенты; т. е. функции $f(x)$ представляет степенной ряд. Формула обращения:

$$\psi(x) = \sum_{n=0}^N \frac{a_n x^n}{b_n}, \quad b_n = (-1)^n \left[\ln 2 + \sum_{m=1}^n \frac{(-1)^m}{m} \right] \quad (20)$$

и вполне можно предположить, что оппонент догадается разложить получаемую графически функцию $f(x)$ в ряд по степеням x . Однако преимуществ от этого он не получит, поскольку далее должен отыскивать b_n фактически путем

перебора вариантов, в надежде уловить предметный смысл сообщения. Но подобные действия не имеют смысла, поскольку равносильны априорному разложению в степенной ряд неизвестной функции $\psi(x)$. Напротив, в арсенале адресата, очевидно, окажется программа эффективного суммирования медленно сходящегося ряда (20).

Пример 3

$$(A\psi)(x) = \psi(x) - \lambda \int_{\rho}^x \frac{g(x)}{g(\xi)} \psi(\xi) d\xi = f(x), \quad (21)$$

где функция $g(x)$ и константы λ, ρ — произвольны. Формула обращения:

$$\psi(x) = f(x) + \lambda \int_{\alpha}^x e^{\lambda(x-\xi)} \frac{g(x)}{g(\xi)} f(\xi) d\xi$$

и, как нетрудно заметить, в (21), аналогично (19), функция $\psi(x)$ находится в явном виде. Однако здесь обозначенную в привязке к (21) проблему особенностей $\psi(x)$ можно преодолеть, если функция $g(x)$ будет содержать достаточно большое количество их прототипов и в арсенале адресата имеется эффективная программа вычисления осциллирующих интеграла. Такой прием, по существу, представляет собой дезинформацию оппонента.

Пример 4

$$(A\psi)(x) = \psi(x) - \int_{\rho}^x g(x) h(\xi) \psi(\xi) d\xi = f(x),$$

где функции $g(x), h(x)$ и константа ρ — произвольны. Формула обращения:

$$\psi(x) = f(x) + \int_{\rho}^x R(x, \xi) \psi(\xi) d\xi,$$

где резольвента

$$R(x, \xi) = g(x) h(\xi) \exp \left[\int_{\xi}^x g(\xi) h(\xi) d\xi \right];$$

здесь прием дезинформации предыдущего примера посредством функции $g(x)$ может быть еще более эффективным за счет дополнительных возможностей, которые предоставляет выбор $h(\xi)$.

Пример 5. Преобразование Стильтьеса

$$(A\psi)(x) = \int_0^{\infty} \frac{\psi(\xi)d\xi}{x+\xi} = f(x); \quad (22)$$

формула обращения:

$$\psi(x) = \frac{1}{2\pi^2 i} \int_{c-i\infty}^{c+i\infty} x^{-\xi} \sin(\pi\xi) g(\xi) d\xi, \quad i^2 = -1; 0 < c < 1, \quad (23)$$

где преобразование Меллина

$$g(\xi) = \int_0^{\infty} x^{\xi-1} f(x) dx;$$

следует отметить конструктивизм преобразования (22) в смысле разрешения главной задачи криптографии по защите информации от оппонента. Естественно, предполагается, что адресат

оснащен программой для проведения вычислений по формуле (23).

Перед оппонентом возникает сложнейшая проблема, даже если он допускает возможность использования интегральных преобразований, поскольку:

- их очень большое количество, причем к каждому нужен сугубо индивидуальный подход;
- протестировать на все из существующих преобразований шифровку $f(x)$ практически невозможно;

- численная реализация интегралов с бесконечными пределами встречает существенные осложнения;

- это также касается практической реализации вычислительных методов в комплексной плоскости;

- аналитические преобразования сопряжены с использованием весьма нетривиального аппарата теории специальных функций.

Пример 6

$$(A\psi)(x) = \int_{-\infty}^{\infty} \frac{\psi(\xi)}{|x-\xi|^{1-\lambda}} d\xi = f(x),$$

$$\int_{-\infty}^{\infty} |f(x)|^p < \infty; 1 < p < 1/\lambda; 0 < \lambda < 1;$$

формула обращения:

$$\psi(x) = \frac{\lambda}{2\pi} \operatorname{tg}\left(\frac{\pi\lambda}{2}\right) \int_{-\infty}^{\infty} \frac{f(x) - f(\xi)}{|x-\xi|^{1+\lambda}} d\xi;$$

можно почти повторить комментарии к предыдущему примеру. Однако обратим внимание, в отличие от него здесь появился параметр λ , допускающий варьирование.

Пример 7

$$(A\psi)(x) = \int_{-\infty}^{\infty} \frac{\psi(\xi)d\xi}{\xi-x} = f(x);$$

формула обращения:

$$\psi(x) = \frac{1}{\pi^2} \int_{-\infty}^{\infty} \frac{f(\xi)d\xi}{\xi-x},$$

где сингулярные интегралы понимаются в смысле главного значения по Коши. Методы вычисления этих интегралов — отдельная тема.

Пример 8. Уравнение Шлемилха

$$(A\psi)(x) = \int_0^{\pi/2} \psi(x \sin \xi) d\xi = f(x);$$

формула обращения:

$$\psi(x) = \frac{2}{\pi} \left[f(0) + x \int_0^{\pi/2} d_\xi f(\xi) d\xi \right]$$

(известно также решение обобщенного уравнения Шлемилха). Подразумевается, что функцию $\psi(z)$ нужно разложить в некоторый ряд по переменной z и затем сделать подстановку $z = x \sin \xi$.

Пример 9. Уравнение Бейтмена

$$(A\psi)(x) = \int_{-1}^1 \frac{\psi(\xi)d\xi}{(1-2x\xi+x^2)^{\alpha+1}} = f(x), \alpha > -1;$$

формула обращения:

$$\psi(x) = (1-x^2)^{\alpha+1/2} \int_0^\pi \gamma(x + \sqrt{x^2-1} \cos \vartheta) \sin^{2\alpha+1} \vartheta d\vartheta,$$

где

$$\gamma(z) = (\alpha+1)f(z) + z d_z f(z); z = x + \sqrt{x^2-1} \cos \vartheta;$$

функции $f(x)$ и $\gamma(z)$ представляют степенные ряды.

Пример 10

$$(A\psi)(x) = \int_{\rho}^x k(\xi)\psi(x)\psi(\xi)d\xi = f(x); \quad (24)$$

формула обращения:

$$\psi(x) = \pm f(x) \left[2 \int_{\varepsilon}^x k(\xi)f(\xi)d\xi \right]^{-1/2}$$

(неоднозначность $\psi(x)$ в данном случае не принципиальна). Однако уравнение (24) является нелинейным, что вносит заметные изменения. В самом деле, дифференцируя его, получаем:

$$k(x)\psi(x) + d_x \psi(x) \int_{\rho}^x k(\xi)\psi(\xi)d\xi = d_x f(x) \quad (25)$$

и если ядру $k(x)$ придать особенности, о которых говорилось в привязке к (21), трудность идентификации тех особенностей, которые объективно присущи функции $\psi(x)$, у оппонента возрастают. Это обусловливается сложностью выражения (25), включая фактор нелинейности.

Пример 11

$$(A\psi)(x) = \int_{\rho}^x k(x, \xi)w(\xi, \psi(\xi))d\xi = f(x); \quad (26)$$

замена

$$w(x) = w(x, \psi(x)) \quad (27)$$

приводит к линейному уравнению

$$\int_{\rho}^x k(x, \xi)w(\xi)d\xi = f(x), \quad (28)$$

что порождает предпосылки неординарно эффективной защиты информации. В самом деле, дифференцируя (28), получаем

$$k(x, x)w(x) + \int_{\rho}^x \partial_x k(x, \xi)w(\xi)d\xi = d_x f(x),$$

однако, в отличие от (19), здесь присутствие функции $w(x)$ практически не представляет опасности, поскольку имеется неограниченный выбор вариантов зависимости (27). Несомненно, он может быть сделан так, что по виду $w(x)$ не удастся выносить какие-либо заключения в отношении сообщения $\psi(x)$. В целом, оптимизация структуры зависимости (27) под углом зрения защиты информации (и в контексте (26)) представляет, по нашему мнению, весьма интересную тему самостоятельного исследования.

5. ИНТЕГРАЛЬНОЕ УРАВНЕНИЕ ФРЕДГОЛЬМА ПЕРВОГО РОДА

Итак, вновь займемся уравнением (7), которое представляет собой совершенно особый объект. Если, например,

$$k(x, \xi) = k(\xi); k(x, \xi) = xk(\xi), \quad (29)$$

шифровка приобретает вид соответственно:

$$f(x) = c_0; f(x) = c_1 x, \quad (30)$$

где c_0, c_1 — некоторые константы. Таким образом, в процессе интегрирования происходит уничтожение информации о функции $\psi(x)$, восстановить которую, в принципе, невозможно. Математически это проявляется в бесконечном множестве решений уравнения (7), ядра и свободные члены которого определяются согласно (29), (30).

Решение уравнения (7) является единственным, если ядро $k(x, \xi)$ замкнуто, что означает:

$$\int_0^1 k(x, \xi) \varphi(\xi) d\xi = 0, x \in [0, 1], \quad (31)$$

лишь в том случае, когда функция $\varphi(x) = 0$; математики дополняют данное равенство понятием «почти всюду» [7, с. 119, 185–187] и, кроме того,

$$\sum_{n=1}^{\infty} a_n^2 \lambda_n^2 < \infty, a_n = \int_0^1 f(\xi) \psi_n(\xi) d\xi,$$

где $\lambda_n; \psi_n(x)$ — характеристические числа и собственные функции ядра $k(x, \xi)$, которое предполагается симметричным, т. е. $k(x, \xi) = k(\xi, x)$. Отметим, что процедуры определения $\lambda_n, \psi_n(x)$ в целом благоприятны для их реализации (отдельная тема, см. [8, п. 10]). Своя специфика возникает, когда ядро $k(x, \xi)$ несимметрично, или же уравнение (31) имеет конечное число нетривиальных решений, однако в настоящем она менее актуальна.

В качестве ядра уравнения (7) подходит, например:

$$k(x, \xi) = \begin{cases} (1-x)\xi, & 0 \leq \xi \leq x; \\ x(1-\xi), & x \leq \xi \leq 1 \end{cases} \quad (32)$$

[8, с. 149]; здесь приведен целый ряд аналогичных выражений. Заметим, что замкнутые ядра могут быть искусственно сконструированы, их множество является неограниченным. Так, вполне подходит решение элементарной задачи об изгибе балки единичной длины и переменного сечения, свободно опертой по краям. В таком случае $k(x, \xi)$ представляет прогиб в сечении с координатой x от единичной силы, приложенной в сечении с координатой ξ .

Однако в чем заключается упомянутая выше особенность интегрального уравнения, с точки зрения, как можно понять, его необычности? Суть в том, что без знания ядра $k(x, \xi)$ восстановление функции $\psi(x)$ из уравнения (7) является невозможным, даже теоретически. Иначе говоря, такой способ шифрования обладает абсолютной надежностью. Казалось бы, исклю-

чительно важный результат для криптографии, ее можно назвать безоговорочная «победа» над криптоанализом. Но где формула обращения интеграла (7), которая была бы аналогичной тем, которые приводились выше? Ответ простой: ее не существует. Тогда должен быть программно-алгоритмический продукт, иначе как же справиться с шифропрограммой адресат?

Все обстоит иначе и ситуация в данной сфере является весьма интересной, поскольку алгоритм и работающая в автоматизированном режиме по данным уравнения (7) программа до настоящего времени, остаются трудно стыкующимися между собой субстанциями. Фундаментальная причина здесь в том, что решение интегрального уравнения Фредгольма первого рода (7) с ядром без благоприятствующих особенностей (для нас они, на данном этапе, неактуальны), представляет собой некорректную задачу. Подразумевается, что малые вариации данных в совершенно неадекватной степени сказываются на решении. Даже вычислив $f(x)$ в аналитическом виде по формуле (7) для ядра (32) и, например, функции $\psi(x) = \sin \omega x$, не удастся восстановить ее обратно, оставаясь в рамках исключительно теперь уже интегрального уравнения (7) из-за округлений значащих цифр в машинной памяти.

Что же делают в такой ситуации? Существует несколько разных подходов, которые хорошо раскрыты в справочнике [9, п. 4]. Наиболее популярная идея состоит в рассмотрении вместо (7) интегрального уравнения:

$$\alpha \psi(x) + \int_0^1 k(x, \xi) \psi(\xi) d\xi = f(x), x \in [0, 1], \quad (33)$$

где $\alpha > 0$ — малый параметр. Формально (33) — весьма хороший объект для численной реализации: интегральное уравнение Фредгольма второго рода, однако, если параметр α не слишком мал. Но в таком случае решение уравнения (33) — совсем другая задача, нежели (7). В общем, «игра» идет на паллиативе выбора α .

Но хуже другое обстоятельство. В не имеющей, наверное, аналогов книге, которая посвящена достаточно объективной апробации большого количества вычислительных методов, Р.П. Федоренко отмечает: «Автором была предпринята попытка использовать этот подход, однако она оказалась неудачной: трудно подобрать нужное значение α . При слишком малых α не получалось гладкого решения, при больших α значение F_0 заметно превосходило минимальное» [10, с. 349–350]. Здесь F_0 — функционал, отвечающий уравнению (33). И далее описывается, как автор выходил из положения с использованием искусственных приемов. Иначе говоря, задача решалась в режиме вычислительного эксперимента с участием человека, что следует подчеркнуть.

Аналогично и А.Ф. Верлань, и В.С. Сизиков по итогам аналитического обзора предлагают свой «способ модельных (эталонных) примеров». «Он заключается в том, что значение α в неко-

тором исходном примере (уравнении, задаче) P выбирается на основе решения вспомогательного (модельного) примера Q (или нескольких модельных примеров) с известным (заданным) точным решением» [9, с. 246–249]. Последующий материал о практической реализации метода свидетельствует, что он также базируется на проведении вычислительного эксперимента, а значит участия человека. Что в этом плохого для криптографии? Суть в том, что существующие методы решения интегральных уравнений Фредгольма первого рода являются не формализованными (о чем профильные источники предпочитают умалчивать), а значит, их нельзя запрограммировать для работы в автоматизированном режиме, т. е. без какого-либо участия адресата. Иначе он превращается в криптоаналитика, или же должен кого-то нанять, что является для нас совершенно неприемлемым, также и с точки зрения вероятных утечек информации.

Претензия (поскольку конкретные вычисления не производились) на разработку в полной мере формализованного алгоритма решения интегральных уравнений Фредгольма первого рода содержится в работе [11]. Идея состоит в том, что причина его некорректности всем понятна: сглаживание информации процедурой интегрирования. Так следует не только лишь иметь это в виду и обговаривать, а благоприятным для последующих выкладок способом смоделировать математически. Предложена модель такого сглаживания, или же — погрешности, которая принимается равной нулю, с искомой функцией $\psi(x)$ в явном виде:

$$\delta(x) = \psi(x) - \lambda \int_{-1}^1 h(x, \xi) \psi(\xi) d\xi = 0, x \in [0, 1], \quad (34)$$

где λ — постоянный параметр; $h(x, \xi)$ — ядро Пуассона в области $x \in [0, 1]$, $\xi \in [-1, 0]$.

Наряду с чем, без использования (34) мы имеем уравнение (7), полностью отвечающее причинно-следственной связи в постановке прямой задачи: изгиб балки; отражение светового луча и т. п. Однако формулировать обратную задачу путем тривиального переименования известной и неизвестной функций в (7), без использования дополнительной информации, является недопустимым. Действительно, процесса «хождения луча назад» не существует. В результате, вообще говоря, нетривиальных преобразований на основе (7) и (34) вычисление функции $\psi(x)$, в предположении ее гармоничности, сводится к решению интегрального уравнения Фредгольма второго рода. Предельный переход $r \rightarrow 1$ в ядре данного уравнения позволяет свести рассматриваемую задачу к решению весьма благоприятной системы линейных алгебраических уравнений относительно коэффициентов ряда Фурье функции $\psi(x)$. Таким образом, она перетекает в более представительный класс функций, квадратично суммируемых на интервале $0 \leq x \leq 1$.

6. ДРУГИЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Выше рассматривались формулы обращения, дающие решения интегральных уравнений в аналитическом виде. Но наряду с этим существуют эффективные алгоритмы численного решения интегральных уравнений [9, пп. 1, 3]. Это касается интегрального уравнения Фредгольма второго рода

$$(A\psi)(x) = \psi(x) - \lambda \int_0^1 k(x, \xi) \psi(\xi) d\xi = f(x), \quad x \in [0, 1], \quad (35)$$

где λ — параметр, отличный от характеристического числа, решение которого, может быть представлено также и через резольвенту:

$$\psi(x) = f(x) + \lambda \int_0^1 R(x, \xi, \lambda) f(\xi) d\xi, x \in [0, 1];$$

следует отметить метод численной реализации $R(x, \xi, \lambda)$, разработанный С.Г. Михлиным [12, п. 12]. В целях защиты информации ядро $k(x, \xi)$ можно задавать с разрывами по переменной x , координаты которых, синхронно с программой адресата, варьирует отправитель. Еще проще, нежели (35), решаются интегральные уравнения Вольтерра второго рода:

$$(A\psi)(x) = \psi(x) - \int_0^x k(x, \xi) \psi(\xi) d\xi = f(x);$$

свои интересные возможности содержит оператор Вольтерра первого рода, существенно искажающий информацию о функции $\psi(x)$, а также аппарат теории нелинейных интегральных уравнений (см. в частности, [7, пп. 4.5, 4.6]). Заметим, что весьма существенные трудности для оппонента может доставить использование ядер $k(x, \xi)$, приводящих к необходимости вычисления интегралов вида

$$\int_0^1 \varphi(x) \exp[\mu w(x)] dx,$$

где μ — большой параметр; функция $w(x)$ является достаточно гладкой. Для этого требуются тонкие методы асимптотического анализа, которые в очень ясной форме представил М.В. Федорюк [13].

И здесь весьма важное обстоятельство, суть которого заключается в следующем. Данные интегральных уравнений задач математической физики, в первую очередь, ядра определяются содержанием рассматриваемых задач предметной области. От свойств упомянутых ядер зависит, в частности, возможность решения нелинейных интегральных уравнений путем последовательных приближений. Однако дешифрование $f(x)$ позволяет задавать ядра из соображений совсем иного толка, вследствие чего могут параллельно решаться вопросы упрощения вычислительных процедур. В общем, сфера защиты информации выдвигает перед теорией интегральных уравне-

ний необычные для нее постановки задач, которые, как нам представляется, заинтересуют специалистов.

Возникает вопрос — не могут ли, наряду с интегральными уравнениями, оказаться полезными для аналогичных целей также и дифференциальные уравнения? Рассмотрим простейший пример для дифференциального уравнения первого порядка

$$d_x \psi + a(x)\psi = f(x), \quad (36)$$

имеющего решение:

$$\psi(x) = \exp\left[-\int a(x)dx\right] \left\{ c + \int f(x) \left[\exp \int a(x)dx \right] dx \right\},$$

где c — константа интегрирования, определяемая из начального условия:

$$c = \frac{\psi(0)}{\exp\left[-\int a(x)dx\right]} - \int f(x) \left[\exp \int a(x)dx \right] dx \Big|_{x=0},$$

а значит, наряду с функцией $f(x)$, адресату нужно знать величину $\psi(0)$, которая зависит от конкретного сообщения. Данное обстоятельство является очень неудобным. Однако мы легко преодолеваем его путем сведения (36) к интегральному уравнению относительно функции $\psi_*(x) = d_x \psi(x)$, откуда с учетом начального условия

$$\psi(x) = \int_0^x \psi_*(\xi) d\xi + \psi(0).$$

Можно ли на этом основании сделать вывод о том, что дифференциальные уравнения для шифрования не нужны? Нет, они могут быть очень полезны, однако в другом контексте. Подразумевается, например, восстановление линейного оператора задачи Штурма — Лиувилля по его спектральным характеристикам [14, с. 9–11]. Как отметил Б.М. Левитан, это могут быть спектры (для разных граничных условий), спектральная функция, данные рассеяния. Применительно к рассматриваемой проблематике, вначале отправитель решает прямую задачу:

$$-d_x^2 u + \psi(x)u = \sigma u, \quad d_x u(0) = d_x u(\pi) = 0 \quad (37)$$

для данной функции $\psi(x)$, которая предполагается непрерывной, по определению собственных значений $\sigma_0, \sigma_1, \dots$

Эту или же аналогичную ей, информацию программное обеспечение адресата использует для решения обратной задачи восстановления $\psi(x)$ на основе математического аппарата [14]. Обратим внимание, здесь присутствует принципиально новый инструмент защиты информации по сравнению с материалом, который изложен выше, а именно: восстановление полезной информации осуществляется путем решения, с использованием глубоко продвинутой математики, весьма содержательной задачи (37). В связи с чем, на оппонента, можно сказать, обрушивается огромный объем информации высокого потенциала, которую, с его позиций, можно назвать «лишней».

Аналогичный инструмент защиты информации предоставляет нам пример из книги [15, с. 4] для уравнения с частными производными. Пусть $\psi(x)$ — непрерывная на всей числовой оси x функция и $u(x, y)$ — решение задачи Коши:

$$[\partial_x + \partial_y + \psi(x)]u = 0, \quad u(x, 0) = \phi(x), \quad (38)$$

где функции $\psi(x); \phi(x)$ даны. Задача определения $u(x, y)$ — корректна, для существования классического решения достаточно потребовать непрерывной дифференцируемости $\phi(x)$. Постановка обратной задачи предполагает отыскание функции $\psi(x)$ из (38) по информации о решении: $u(0, y) = \phi(y)$. Если $\phi(x) \neq 0$ в рассматриваемой области, то решение этой задачи однозначно. Для его существования необходимо и достаточно выполнение условий: функция $\phi(y)$ — непрерывно дифференцируема; $\phi(y)/\phi(y) > 0; \phi(0) = \phi(0)$. В таком случае решение имеет вид

$$\psi(x) = -\frac{d}{dx} \ln \frac{\phi(x)}{\phi(x)}.$$

В.Г. Романов рассмотрел также целый ряд гораздо более сложных задач, с использованием решений которых мы могли бы весьма эффективно загружать оппонента потоками лишней информации. К ним, в частности, относятся обратные задачи определения плотности тепловых источников и коэффициента диффузии [15, пп. 6.1, 6.2]. В таком же аспекте очень эффективен аппарат парных уравнений, на высоком уровне представленный Н.А. Вирченко [16]. В самом деле, как подлежащая шифрованию функция $\psi(x)$, так и шифровка $f(x)$ подвергаются здесь эшелонированному воздействию, можно сказать, информационно супернасыщенных операторов. Причем, вновь на передний план выходят процедуры интегрирования. Приведем лишь сравнительно несложный пример [6, с. 459].

Решение парного интегрального уравнения

$$\int_0^\infty g(\xi) J_0(x\xi) \psi(\xi) d\xi = f(x), \quad 0 < x < a; \quad (39)$$

$$\int_0^\infty \xi J_0(x\xi) \psi(\xi) d\xi = 0, \quad a < x < \infty, \quad (40)$$

где функция $g(x)$ — дана; $J_0(x)$ — функция Бесселя нулевого порядка, имеет вид

$$\psi(x) = \int_0^a \phi(\xi) \cos(x\xi) d\xi; \quad (41)$$

функция $\phi(x)$ определяется из интегрального уравнения Фредгольма второго рода:

$$\phi(x) - \frac{1}{\pi} \int_0^a K(x, \xi) \phi(\xi) d\xi = \phi(x), \quad 0 < x < a, \quad (42)$$

симметричное ядро $K(x, \xi)$ и свободный член $\phi(x)$ даются выражениями

$$K(x, \xi) = 2 \int_0^\infty [1 - g(\vartheta)] \cos(x\vartheta) \cos(\xi\vartheta) d\vartheta; \quad (43)$$

$$\phi(x) = \frac{2}{\pi} \frac{d}{dx} \int_0^x \frac{\xi f(\xi)}{\sqrt{x^2 - \xi^2}} d\xi. \quad (44)$$

Обратим внимание на следующие моменты:

- по формуле (39) отправитель, казалось бы, аналогично предыдущему (см. пп. 3, 4), вычисляет $f(x)$, шифруя сообщение $\psi(x)$, $0 < x < a$, однако с выбором функции $g(x)$, а также произведения $g(x)\psi(x)$, $x > a$, возникает неопределенность;

- очевидно, для существования интегралов (39), (40) на функции $\psi(x)$, $g(x)$, $x > a$ должны налагаться некоторые ограничения;

- программа адресата восстанавливает $\psi(x)$ по формуле (41) что, как и решение интегрального уравнения (42), вообще говоря, не должно вызывать принципиальных осложнений, однако, многое определяется выбором функции $g(x)$, это касается также интеграла (43),

- весьма непросто, вследствие сингулярности, без предварительной подготовки, является вычисление функции (44);

- резюмируя обозначенные моменты, можно сделать вывод о том, что нет у оппонента малейшего шанса для идентификации сообщения $\psi(x)$, $0 < x < a$, если ему не известна постановка задачи (39), (40).

7. ИЗ СОВРЕМЕННОЙ АЛГЕБРЫ В НЕПРЕРЫВНЫЙ АНАЛИЗ: ОБРАТНО (НАЗАД)

Конечно, под «алгеброй» здесь подразумеваются алгебраическая геометрия и алгебраическая теория чисел, лежащие, как известно, в основе АК. То есть, это разделы современной алгебры, развитию которых способствовали теория чисел, алгебра, а также, в первую очередь, наверное, анализ, о чем свидетельствует приведенная ниже выдержка, в их классическом понимании. В этой связи интересно пояснение С.М. Никольского: «Математический анализ — часть математики, в которой функции и их обобщения изучаются методами пределов. Понятие предела тесно связано с понятием бесконечно малой величины, поэтому можно также говорить, что математический анализ изучает функции и их обобщения методом бесконечно малых. ... В математическом анализе исходят из определения функции по Лобачевскому и Дирихле. Если каждому x из некоторого множества F чисел в силу количественного закона приведено в соответствие число y , то этим определяется функция $y = f(x)$ от одного переменного x » (МЭ, 1982. — Т. 3. — С. 591).

Большой интерес представляют соображения Ф.А. Медведева о взаимосвязи анализа с теорией функций, поскольку последняя в значительной мере повлияла на облик АК (см. ниже): «Если исключить из классического анализа теорию дифференциальных уравнений и теорию функций комплексного переменного, выделившихся в огромные самостоятельные отрасли

математического знания, то можно сказать, что теория функций действительного переменного есть просто расширенный, углубленный и обобщенный математический анализ» [17, с. 9]. И далее: «Тесная взаимосвязь анализа и теории функций порой неувидимые переходы их друг в друга приводят к вопросу о взаимоотношении этих двух математических дисциплин. Действительно ли это разные науки, и если да, то чем они отличаются одна от другой?

Первое бросающееся в глаза отличие заключается в отсутствии в явном виде теоретико-множественных представлений в классическом анализе и привлечения их в очень большом объеме к теории функций. Исходный объект анализа — функция — всегда определена на некоторой нерасчлененной части области — отрезке, прямой, куске плоскости, объеме пространства. Напротив, в теории функций она вообще задается на некотором множестве точек, и ее свойства существенно зависят от характера множества, на котором она задана; естественно поэтому, что изучению функций здесь предпосылается изучение множеств. Более того, такое предпослание необходимо и потому, что решение многих вопросов теории функций зависит от решения теоретико-множественных вопросов.

Укажем только один пример. В классическом анализе для того, чтобы решить вопрос интегрируема или нет заданная функция, нужно было попросту вычислить ее интеграл, или установить, что рассматриваемая функция принадлежит определенному классу функций, для которых определено понятие интеграла, причем сам этот класс вводится способом, не апеллирующим к теории множеств. Напротив, для того, чтобы ответить на вопрос об интегрируемости функции по Риману, необходимо и достаточно узнать, равна ли нулю мера множества точек ее разрывов. Так обстоит дело в большинстве вопросов теории функций. И не случайно еще на заре зарождения современной теории функций один из ее основателей Р. Бэр, писал в 1899 г.: «... в том порядке идей, которыми мы занимались, все проблемы относительно функций сводятся к вопросам, относящимся к теории множеств; и в той мере, в какой эти последние продвинуты или могут быть продвинуты вперед, в такой же мере можно решить более или менее полно данную проблему» [17, с. 10].

В первой половине 1930-х гг., появились два курса под одинаковым названием «Теория функций», которые приобрели большую известность, став классическими [18, 19]. При этом авторы очень различно трактуют содержание предмета теории функций. Объединяет их, пожалуй, лишь отсутствие теоретико-множественных конструкций. У Е. Титчмарша в чистом виде анализ с охватом широкой проблематики, по которой даны разъяснения наиболее тонких моментов. В общем, корреляция ИК с методологией [18] очевидна. В этом смысле материал [19] можно назвать противоположным, поскольку здесь преимущественно комплексный анализ в контексте

его геометрических интерпретаций. Во второй части [19] рассмотрены эллиптические функции, а также кривые, причем на данный материал ссылаются в качестве его идейной предтечи алгебраической геометрии. «Эллиптическая кривая является истоком большей части современной алгебраической геометрии. Но исторически теория эллиптических кривых возникла как часть анализа — «теории эллиптических интегралов и эллиптических функций» (МЭ, 1985. — Т. 5. — С. 979). Таким образом, существует прямой путь к АК от раздела классического анализа через теорию функций, в смысле [19].

Другая основа АК — алгебраическая теория чисел, естественно, обуславливается тем, что традиционный инструмент шифрования — целое число. Как представляется, здесь АК в большей мере адаптировалась к уже сложившейся теории. Однако весьма интересное обстоятельство заключается в том, что из классической алгебры можно также перейти к непрерывному анализу, включая ИК. Только лишь следует взять подходящий для этого ее раздел, а именно — линейную алгебру. Напомним, что выше (п. 1) мы уже продемонстрировали предельный переход от конечного алгебраического ряда к анализу и ИК, следуя [5]. Однако сейчас обратим внимание на теорию Фредгольма, в которой вывод интегрального уравнения, а также построение общей теории его решения осуществляются путем предельного перехода к бесконечной системе линейных алгебраических уравнений.

Как отметил И.И. Привалов: «Полное исчерпывающее решение задачи было дано Фредгольмом в 1904 г., и эта работа Фредгольма содержит самое выдающееся открытие начала XX в. в области анализа, после которого быстро развивается теория интегральных уравнений. Основная идея Фредгольма состоит в том, что интегральное уравнение (35) рассматривается как предельное состояние для системы n линейных алгебраических уравнений с n неизвестными, когда n неограниченно возрастает» [20, с. 39]. По мнению, Э. Гурса, полученный Фредгольмом результат о том, что «резольвента есть частное от деления двух функций, целых относительно λ , ..., т. е. мероморфная функция параметра λ , является очень существенным, и предвидеть его заранее было бы трудно» [21, с. 51].

Приведем некоторые соображения:

- как АК, так и ИК имеют истоки в классической алгебре, однако — разных ее разделах (в первом случае — это многочлены и группы, во втором — системы линейных уравнений);

- АК также имеет одним из своих истоков классический анализ (эллиптические функции), тогда как ИК полностью, и очень органично, находится в его сфере;

- напротив, АК на переднем крае математики (современная алгебра), а соответственно ей присущи большая степень абстракции, сложность для восприятия и т. п. аспекты;

- однако при этом АК осталась «алгеброй», которая оперирует с целыми числами, ставя перед криптоанализом задачи дискретного характера (т. е., в них конечное число неизвестных);

- ИК, напротив, оперирует с функциями, за каждой из которых неограниченное количество информативных, скажем так, признаков — значений в точках непрерывного аргумента.

Вместе с тем, функции можно рассматривать и как символы. В самом деле, за символом, например, $\sin$ располагается неограниченное множество его значений, отвечающих бесконечно малому приращению аргумента ωx на интервале $0 \leq x \leq 1$. Хотя и ωx можно трактовать как функцию x . Причем, преобразуется до полной неузнаваемости (для оппонента) как единственный символ, так и их сложные композиции. Соответственно значения функции, например, $\sin \omega x$, после дешифрования путем преобразований, зачастую, также в категориях, исключительно символов, адресат может определять с высокой степенью точности. Подробнее раскроем принципиальное преимущество ИК, заключающееся в том, что данные, которые подлежат шифрованию, включая буквы и обозначения, можно представлять функциями непрерывного аргумента.

У них, во-первых, радикально более широкий спектр возможных преобразований, по сравнению с наборами целых чисел АК. И, во-вторых, в ИК мы имеем качественно отличительную особенность своего рода экономичности, поскольку преобразования происходят с объектами высоко-информационной насыщенности, а именно — функциями непрерывного аргумента, которые выражаются символам. Вследствие этого, они ничтожно малы в машинной памяти. С другой стороны, данные символы можно трактовать и в качестве операторов, воздействующих на функции, причем даже когда мы имеем графики, поскольку они разлагаются в ряды, представляющие собой аналитические выражения. Соответственно в машинной памяти не требуется хранить большие массивы чисел, по ходу реализации алгоритма их генерируют операторы. Подобного рода возможностей абсолютно лишена существующая криптография.

В заключение хотелось бы отметить, что представленный материал, конечно, заслуживает того, чтобы в совершенно ином ракурсе оценить потенциал криптологии в целом. Причем, его содержание является, в общем-то, несложным, хотя и охватывает широкий спектр позиций, а идейная сторона, как говорится, лежала на поверхности. В этом отношении мы уже выражали недоумение (введение). Однако, глядя на ситуацию с другой стороны, приведем определения: «Алгебра — часть математики, посвященная изучению алгебраических операций» (МЭ, 1977. — Т. 1. — С. 114). «Алгебраическая операция — n -арная операция на множестве A — отображение $\omega: A^n \rightarrow A$ n -й декартовой степени множества A в само множе-

ство A . Число n называется арностью алгебраической операции. ...В XX в. появилось понятие бесконечно местной операции, т. е. отображение $\omega: A^\alpha \rightarrow A$, где α — произвольное кардинальное число» (там же, с. 159).

Имеется в виду следующее. Если человек действительно мыслит категориями теории множеств, да еще и разделяет мрачное, как нам представляется, «пророчество» Бэра (см. цитату [19] выше), то для такой ментальности наш материал, наверное, окажется чужеродным. Кстати, следует заметить, что математическая «современность» для криптографии далеко не главный показатель. На первом месте здесь, очевидно, должна быть коммерческая эффективность, а также и аспекты социально-политического характера. В общем, мы, как смогли, постарались пояснить название раздела о том, почему целесообразно вернуться назад (подразумевается развитие математической науки во времени) — в сферу непрерывного анализа.

ВЫВОДЫ

1. Как показал информационный поиск, аппарат непрерывного анализа не привлекают для целей криптографической защиты, что представляется удивительным с позиций следующего подхода: шифрование посредством интегрирования функции, которая может олицетворять хотя бы и число; дешифрование — путем решения интегрального уравнения.

2. Аналитический метод криптографической защиты, с помощью перемножения целочисленных матрицы и вектора, удается использовать лишь в случае очень малой размерности, однако, казалось бы, парадокс — в условиях ее неограниченности мы получаем интегральное уравнение Фредгольма первого рода, что свидетельствует в пользу непрерывного анализа.

3. Поскольку подходящих для криптографической защиты интегральных операторов весьма много, то дешифрование, в автоматизированном режиме, целесообразно производить для большого количества номеров настроек, которые сообщаются адресату, хотя бы и открыто, прямого доступа к программному обеспечению он иметь не должен.

4. В целом ряде случаев, как интегрирование функций, так и их восстановление по формулам обращения удается производить в замкнутом виде, более того, вручную, причем, как показывают конкретные примеры, шифрограммы совсем не напоминают исходные сообщения, а значит, у криптоанализа возникают весьма серьезные проблемы.

5. Приведен ряд интегралов, с формулами обращения в аналитическом виде, на основании которых, учитывая их последовательные применения, различного рода комбинации, а также другие приемы, становится совершенно очевидным, что предлагаемый метод криптографической защиты ставит перед криптоанализом, по нашему мнению, практически неразрешимые задачи.

6. Интегральное уравнение Фредгольма первого рода, вследствие своей некорректности, представляет особый интерес, поскольку, не зная ядра, криптоаналитик не в силах выполнить дешифрование даже теоретически, однако, алгоритмы его решения не могут работать без участия человека (производится вычислительный эксперимент); преодолению данного обстоятельства посвящена наша публикация 2005 года.

7. Для целей криптографической защиты можно «заглянуть» также и в другие разделы анализа, в частности, это — задачи математической физики, решения которых, вследствие своей содержательности, могут преподносить криптоаналитику большой объем лишней для него информации, в условиях, когда сообщение адресату представляет, например, какой-нибудь коэффициент теплопроводности.

8. Истоком алгебраической геометрии, на которой в значительной мере базируется криптология современного формата, является математический анализ и поскольку использование функций непрерывного аргумента имеет в процедурах шифрования — дешифрования неоспоримые преимущества над дискретностью, то следует, по нашему мнению, образно выражаясь, «вернуться назад» (т. е., в непрерывный анализ).

Литература

- [1] Крыжановский А.В. Средства обеспечения информационной безопасности в сетях передачи данных: задачи и методические указания / А.В. Крыжановский, Н.В. Киреева, В.В. Пугин. — Самара: Поволжская государственная академия телекоммуникаций и информатики. — 2008. — 61 с.
- [2] Грегори Р. Безошибочные вычисления. Методы и приложения / Р. Грегори, Е. Кришнамурти. — М.: Мир, 1988. — 208 с.
- [3] Форсайт Дж. Численное решение систем линейных алгебраических уравнений / Дж. Форсайт, К. Молер. — М.: Мир, 1969. — 168 с.
- [4] Форсайт Дж. Машинные методы математических вычислений / Дж. Форсайт, М. Малькольм, К. Моулер. — М.: Мир, 1980. — 280 с.
- [5] Кук Р. Бесконечные матрицы и пространства последовательностей / Р. Кук. — М.: Физматгиз, 1960. — 472 с.
- [6] Полянин А.Д. Справочник по интегральным уравнениям / А.Д. Полянин, А.В. Манжиров. — М.: Физматлит, 2003. — 608 с.
- [7] Трикоми Ф. Интегральные уравнения / Ф. Трикоми. — М.: Изд-во иностр. лит., 1960. — 300 с.
- [8] Краснов М.Л. Интегральные уравнения / М.Л. Краснов, А.И. Киселев, Г.И. Макаренко. — М.: Наука, 1976. — 216 с.
- [9] Верлань А.Ф. Интегральные уравнения: методы, алгоритмы, программы. Справочное пособие / А.Ф. Верлань, В.С. Сизиков. — К.: Наукова думка, 1986. — 544 с.
- [10] Федоренко Р.П. Приближенное решение задач оптимального управления / Р.П. Федоренко. — М.: Наука, 1978. — 488 с.

- [11] Перчик Е. Методология синтеза знаний: преодоление фактора некорректности задач математического моделирования / www.pelbook.narod.ru (2-я ред.)
- [12] Михлин С.Г. Некоторые вопросы теории погрешностей / С.Г. Михлин. — Л.: Изд-во Ленингр. ун-та, 1988. — 334 с.
- [13] Федорюк М.В. Асимптотика: Интегралы и ряды / М.В. Федорюк. — М.: Наука, 1987. — 544 с.
- [14] Левитан Б.М. Обратные задачи Штурма — Лиувилля / Б.М. Левитан. — М.: Наука, 1984. — 240 с.
- [15] Романов В.Г. Обратные задачи математической физики / В.Г. Романов. — М.: Наука, 1984. — 264 с.
- [16] Вірченко Н.О. Парні (N -арні) інтегральні рівняння / Н.О. Вірченко. — К.: Задруга. — 2009. — 475 с.
- [17] Медведев Ф.А. Очерки истории теории функций действительного переменного / Ф.А. Медведев. — М.: Наука, 1975. — 248 с.
- [18] Титчмарш Е. Теория функций / Е. Титчмарш. — М.: Наука, 1980. — 465 с.
- [19] Гурвиц А. Теория функций / А. Гурвиц, Р. Курант. — М.: Наука, 1968. — 648 с.
- [20] Привалов И.И. Интегральные уравнения / И.И. Привалов. — М.; Л.: ОНТИ, 1937. — 248 с.
- [21] Гурса Э. Курс математического анализа / Э. Гурса. — М.; Л.: Гостехиздат, 1934. — Т. 3. — Ч. 2. — 320 с.

Поступила в редколлегию 22.06.2014



Громыко Игорь Алексеевич, кандидат технических наук, доцент, профессор кафедры безопасности информационных систем и технологий факультета компьютерных наук Харьковского национального университета имени В. Н. Каразина. Научные интересы: построение базовых основ информационной безопасности,

разработка Всеобщей парадигмы защиты информации в Украине, разработка теоретических основ и действующих базовых функциональных элементов для принципиально новой квантовой системы дистанционного получения информации в акустическом диапазоне с поверхностей помещений; исследования материальных процессов субъектного преодоления пространственно-временного континуума с целью получения ретро и экспресс-информации; исследование возможности локального ограничения процесса распространения акустических колебаний в воздушном пространстве.

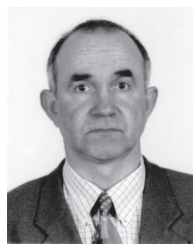


Броншпак Геннадий Кимович, кандидат экономических наук, председатель совета директоров АО «Фудзилэнд». Научные интересы: задачи и методы экономико-математического моделирования; системный анализ на уровне объединения предприятий.



Перчик Евгений Львович, кандидат технических наук, старший научный сотрудник, начальник информационно-аналитического отдела АО «Научно-технологический институт транскрипции, трансляции и репликации». Научные интересы: методы математического модели-

рования; задачи математической физики; теория интегральных уравнений.



Доценко Сергей Ильич, кандидат технических наук, доцент, профессор кафедры электроснабжения и энергетического менеджмента Харьковского национального технического университета сельского хозяйства имени Петра Василенка. Научные интересы: теория и практика энергетического менеджмента, теория деятельности, теория функциональных систем, информационные технологии интеграции предприятия.

УДК 517.9.621

Криптография нового поколения: интегральные уравнения как альтернатива алгебраической методологии / Г.К. Броншпак, И.А. Громыко, С.И. Доценко, Е.Л. Перчик // Прикладна радіоелектроніка: наук.-техн. журн. — 2014. — Том 13. — № 3. — С. 337–349.

Показано переваги використання в криптографії положень математичного аналізу, зумовлені властивістю функцій неперервного аргументу. Як такі можуть виступати як попередньо представлені рядками графіки, таблиці, відеозображення, так і букви, числа, символи, відповідно яким поставлені, наприклад, синуси різної амплітуди. Шифрування проводиться шляхом інтегрування функцій, дешифрування — шляхом розв'язання інтегральних рівнянь. Наведено приклади реалізації даних процедур в аналітичному вигляді. Різноманітні варіанти таких перетворень, включаючи їх застосування в комбінаціях, ставить перед криптоаналізом практично нездоланні проблеми. Розглянуто можливість використання для криптографічного захисту відомих розв'язань задач математичної фізики. Проаналізовано сутність високої ефективності шифрування, що базується на залежності функцій від необмеженого числа інформативних ознак.

Ключові слова: криптографія, неперервний аналіз, інтегрування, інтегральні рівняння, формули обернення.

Бібліогр.: 21 найм.

UDC 517.9.621

Cryptography of a new generation: integral equations as an alternative of algebraic methodology / G.K. Bronshpak, I.A. Gromyko, S.I. Dotsenko, E.L. Perchik // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 337–349.

The advantages of using points of mathematical analysis in cryptography due to the properties of continuous argument functions are shown. Pre-series presented graphs, tables, videos and letters, numbers, symbols may act in their capacity, for example, sinuses of different amplitude are placed in correspondence with. Encryption is performed by integration of functions, decryption is realized by solving integral equations. Examples of realizing these procedures in an analytical form are provided. A variety of options of such transformations, including their use in combinations, poses almost insurmountable cryptanalytic problems. The possibility of using the known solutions of problems of mathematical physics for cryptographic protection is considered. The essence of high performance encryption based on the dependence of the functions upon an unlimited number of informative features is analyzed.

Keywords: cryptography, continuous analysis, integration, integral equations, inversion formulae.

Ref.: 21 items.

МЕТОДОЛОГІЯ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

О.В. ОНАЦЬКИЙ

Розглядається методологія створення комплексної системи захисту інформацій відповідно до вимог законодавства України. Наведено порядок та етапи створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах. Розглядаються основні питання, пов'язані зі створенням комплексів технічного захисту інформації на об'єктах інформаційної діяльності.

Ключові слова: комплексна система захисту інформації, інформація з обмеженим доступом, автоматизована система, інформаційно-телекомунікаційна система.

ВСТУП

Інформація, будучи продуктом діяльності, виступає як власність держави, підприємств, установ, організацій та громадян, і, як об'єкт власності, вимагає захищеності. Проте проблема захисту інформації не зводиться тільки до захисту прав її власників, але і містить в собі такий важливий аспект, як захист прав громадян на вільний доступ до відомостей, гарантований Конституцією. Основи захисту інформації розробляються органами державної влади, виходячи з умов забезпечення інформаційної безпеки зокрема і національної безпеки України в цілому. Відповідно до ст. 20, 21 Закону України "Про інформацію", вся інформація за порядком доступу поділяється на відкриту та інформацію з обмеженим доступом (ІзОД). ІзОД є конфіденційна, таємна та службова інформація [1]. Такий розподіл по режимах доступу здійснюється винятково на підставі ступеня конфіденційності інформації. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [1].

Оскільки в умовах інформатизації країни [2], розвитку інформаційних технологій, інформаційні ресурси (сукупність документів у інформаційних системах [2]) формуються у всіх сферах діяльності, і насамперед: в політичній, військовій, економічній, науково-технічній, тому інформаційну безпеку слід розглядати як комплексний показник національної безпеки. Цим визначається її важливе місце і одна з провідних ролей в системі національної безпеки країни в сучасних умовах [3].

Згідно із Законом України "Про захист персональних даних" об'єктами захисту є персональні дані, які обробляються в базах персональних даних. Персональні дані за режимом доступу є ІзОД [4]. Відповідно до ст. 8 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" "Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з

підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством" [5].

Відповідно до вимог законодавства України [1...8], для забезпечення конфіденційності, доступності, цілісності та спостереженості зазначеної інформації в кожній автоматизованій системі (АС) має створюватися комплексна система захисту інформації (КСЗІ).

Над вирішенням проблем у сфері захисту інформації, зокрема у проведенні інженерно-технічних заходів, працюють сучасні дослідники, такі як В.В. Домарев, А.А. Хорев, Г.Ф. Конахович, А.О. Торокін та ін. Варіант захисту мовної інформації зі створенням комплексів технічного захисту інформації на об'єктах інформаційної діяльності розглянуто в роботі [9], дослідження порядку та особливості проведення державної експертизи комплексних систем захисту інформації в інформаційно-телекомунікаційних системах пропонується в роботі [10], принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах розглянуто в [11].

Аналіз робіт, зазначених авторів, свідчить, що ними розглядаються варіанти побудови комплексу захисту мовної інформації від витоку технічними каналами [9, 11], порядок проведення державної експертизи КСЗІ [10], але в ній не враховані усі вимоги державних нормативних документів у галузі технічного захисту інформації, які регламентують порядок створення не тільки комплексу технічного захисту інформації на об'єкті інформаційної діяльності (ОІД), але комплексу засобів захисту від несанкціонованого доступу.

Метою статті є здійснити повний аналіз створення комплексної системи захисту інформацій відповідно до вимог законодавства України.

1. СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Комплексна система захисту інформації — взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [12]. Порядок проведення робіт

із створення КСЗІ в інформаційно-телекомунікаційній системі (ІТС) розглянуто в НД ТЗІ 3.7-003-05, а також вимоги в частині організації робіт із захисту інформації та порядку створення КСЗІ в ІТС, розвиває основні положення ДСТУ 3396.0-96, ДСТУ 3396.1-96, НД ТЗІ 3.6-001-2000, НД ТЗІ 3.7-001-07 та інших нормативних документів технічного захисту інформації (НД ТЗІ). Для організації робіт зі створення КСЗІ в ІТС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД ТЗІ 1.4-001-2000.

КСЗІ складається з організаційних і інженерних заходів, комплексу технічного захисту інформації (КТЗІ) (захист від витоку інформації технічними каналами) та комплексу засобів захисту (КЗЗ) від несанкціонованого доступу (НСД) до ІзОД.

Організаційні заходи є обов'язковою складовою побудовою будь-яких КСЗІ. Організаційні заходи включають в себе:

- створення концепції інформаційної безпеки;
- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб НСД до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів.

Інженерно-технічні заходи — сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити. У рамках проведення інженерно-технічних заходів, можуть бути встановлені:

- система охоронної сигналізації;
- система відеоспостереження;
- система пожежної сигналізації;
- система автоматичного пожежогасіння;
- система охорони периметра;
- система контролю управління доступом;
- система збору та обробки інформації.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань та наведень (ПЕМВН), акустoeлектроічні та інші канали;
- несанкціонованих дій та НСД до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскуванню під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін.;
- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Створення КТЗІ від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю (1, 2, 3 категорій об'єктів згідно з ТПКО-95 [13]), або коли необхідність цього визначено власником інформації [14].

Впровадження КЗЗ здійснюється в усіх ІТС, де обробляється інформація, що є власністю держави, яка належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС.

Виділяються наступні етапи створення КСЗІ, які показані на рис. 1.

2. ЕТАПИ СТВОРЕННЯ КСЗІ

1. Формування загальних вимог до КСЗІ в ІТС.

1.1. Обґрунтування необхідності створення КСЗІ. На цьому етапі проводиться аналіз нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями.



Рис. 1. Етапи створення комплексної системи захисту інформації

Визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів.

Результат роботи – наказ про створення КСЗІ; положення про службу захисту інформації; проекти посадових інструкцій; наказ про встановлення контрольованої зони; план заходів на рік; наказ про створення комісії для проведення категоріювання ІТС, приміщення; акт проведення категоріювання ІТС, приміщення; наказ про створення комісії з проведення обстеження ІТС.

1.2. Обстеження середовищ функціонування ІТС. При обстеженні середовищ функціонування ІТС необхідно проаналізувати всі складові (рис. 2): обчислювальну систему; фізичне середовище; середовище користувачів; оброблювану інформацію і технологію її обробки.

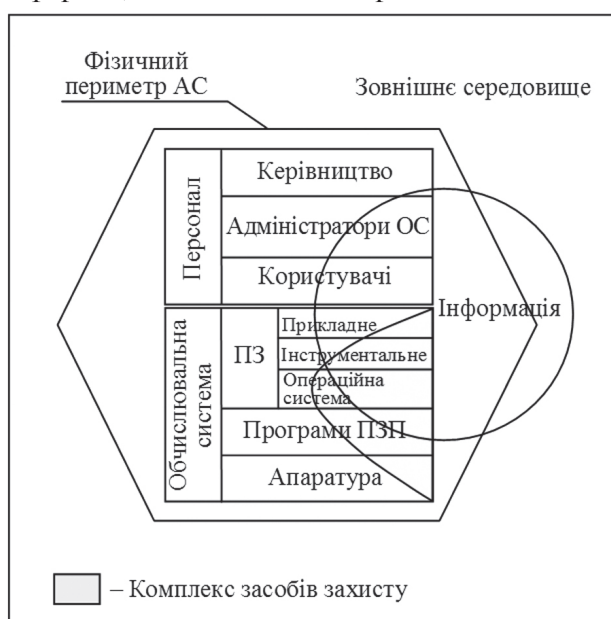


Рис. 2. Середовище функціонування ІТС

Порядок проведення обстеження має відповідати ДСТУ 3396.1-96. Результати обстеження середовищ функціонування ІТС оформляються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС, який розробляється згідно з НД ТЗІ 1.4-001-2000. За результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001-2000, НД ТЗІ 2.5-007-07, НД ТЗІ 2.5-008-02, НД ТЗІ 2.5-010-03 щодо класифікації об'єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000 та НД ТЗІ 1.6-003-04.

Результат роботи – акт обстеження ІТС (містить опис, принципи побудови й архітектуру ІТС); перелік об'єктів захисту ІТС; модель порушника; модель загроз інформації.

1.3. Формування завдання на створення КСЗІ. На цьому етапі визначається завдання захисту інформації в ІТС, мета створення КСЗІ, варіант вирішення задач захисту, основні напрями забезпечення захисту, загальна структура та склад КСЗІ, засобів захисту інформації; здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз. Здійснюється оформлення звіту про виконання робіт цієї стадії та оформлення заявки на розробку КСЗІ – технічного завдання (ТЗ) на створення КСЗІ.

Результат роботи – затверджений акт обстеження та перелік об'єктів захисту.

2. Розробка політики безпеки інформації в ІТС.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002-99 та рекомендаціями НД ТЗІ 1.4-001-2000. Політику безпеки рекомендується оформляти у вигляді окремого документа – плану захисту інформації.

Результат роботи – план захисту інформації: модель загроз інформації, завдання на створення КСЗІ, політика захисту інформації в ІТС.

3. Розробка технічного завдання на створення КСЗІ.

Технічне завдання на створення КСЗІ в ІТС є організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію у складі ІТС. Розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження має відповідати НД ТЗІ 3.7-001-99 та ГОСТ 34.602-89.

Результат роботи – технічне завдання на створення КСЗІ, яке погоджується з Державною службою спеціального зв'язку та захисту інформації України (ДССЗІ України), після цього затверджується підприємством.

4. Розробка проекту КСЗІ.

Проект КСЗІ розробляється на підставі та відповідно до ТЗ на створення ІТС. Проект КСЗІ виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робочий проект. Технічний проект на створення КСЗІ є комплектом документів, у який входить частина документів розроблених на попередніх етапах і ряд нових документів, у яких описано, як саме створюватиметься, експлуатуватиметься та модернізуватиметься КСЗІ.

Результат роботи – технічний проект на створення КСЗІ; технічна, робоча та експлуатаційна документація КСЗІ в ІТС.

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС.

5.1. Підготовка КСЗІ до введення в дію. Проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС.

5.2. Навчання користувачів. Проводиться навчання користувачів ІТС усіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ та ін.) в частині, що їх стосується, основним положенням документів плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, перевірка їх умінь користуватися впровадженими технологіями захисту інформації і реєстрація результатів навчання.

Результат роботи — ознайомлення користувачів з відповідними інструкціями.

5.3. Комплектування КСЗІ. Забезпечується отримання продукції (засобів захисту інформації, матеріалів, обладнання та ін.) від постачальників та співвиконавців робіт. Приймається рішення щодо підготовки до проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проектування КСЗІ не мали відповідних сертифікатів або експертного висновку, а також порядку проведення такої оцінки під час державної експертизи КСЗІ.

5.4. Будівельно-монтажні роботи. Роботи цього етапу виконуються під час переобладнання існуючих або при будівництві нових спеціалізованих споруд (приміщень), призначених для розміщення технічних засобів ІТС та персоналу, сховищ матеріальних носіїв інформації. Під час проведення будівельно-монтажних робіт враховуються вимоги технічного завдання на створення КСЗІ в ІТС.

5.5. Пусконаладжувальні роботи. Метою пусконаладжувальних робіт є: монтаж обладнання і атестація комплексу технічного захисту інформації від витоків технічними каналами; встановлення і налагодження КЗЗ; перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії. Монтаж основних технічних засобів (ОТЗ) ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

5.6. Попередні випробування. Випробування — експериментальне визначення кількісних та/або якісних характеристик властивостей об'єкта експертизи за результатом впливу на нього під час його функціонування [15]. Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію. Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

Результат роботи — програма та методика попередніх випробувань; протокол проведення попередніх випробувань; акт завершення попередніх випробувань КСЗІ ІТС.

5.7. Дослідна експлуатація. Під час дослідної експлуатації КСЗІ: відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, роз-

межування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів; співробітники служби захисту інформації (СЗІ) та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів; здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ; здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

Результат роботи — встановлення необхідних технічних або криптографічних засобів захисту інформації; засобів фізичного захисту елементів ІТС (встановлюється необхідне обладнання й програмне забезпечення, засоби контролю доступу, охоронна й пожежна сигналізація) і т.д. Пакет документів “Експлуатаційна документація на КСЗІ”: інструкції експлуатації КСЗІ і її елементів; процедури регламентного обслуговування КСЗІ; правила й положення з проведення тестування й аналізу роботи КСЗІ. Акт приймання КСЗІ в ІТС у дослідну експлуатацію, акт завершення дослідної експлуатації КСЗІ в ІТС.

За результатом випробування КСЗІ робиться висновок щодо можливості подання КСЗІ на державну експертизу.

5.8. Державна експертиза КСЗІ. Відповідно до п.1.4 Положення про Державну експертизу в сфері технічного захисту інформації КСЗІ підлягає обов'язковій перевірці на відповідність вимогам чинних нормативних документів з технічного захисту інформації в ІТС [14]. Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІТС. Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам нормативної документації із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію. Державна експертиза КСЗІ в ІТС проводиться згідно з Положення про державну експертизу в сфері технічного захисту інформації та НД ТЗІ 2.6-001-11. Об'єктами експертизи (ОЕ) можуть бути як КСЗІ, які є невід'ємною складовою частиною ІТС, так і окремі засоби технічного захисту інформації від НСД, у тому числі захищені від НСД компоненти обчислювальної системи [15].

Державна експертиза КСЗІ, передбачає виконання таких етапів експертних робіт:

- попереднє ознайомлення з ОЕ;
- поглиблене обстеження ОЕ;
- розроблення програми проведення експертизи КСЗІ;
- розроблення методики проведення експертизи КСЗІ;
- проведення експертних випробувань та досліджень ОЕ за розробленими програмою та методикою;

— документування та затвердження результатів експертизи.

Результат роботи — програма та методика проведення експертизи КСЗІ; особлива думка експерта; протокол випробувань; атестат відповідності та експертний висновок.

6. Супроводження КСЗІ.

Виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійного і післягарантійного технічного обслуговування засобів захисту інформації.

В загальному вигляді порядок створення КСЗІ в ІТС схематично відображено на рис. 3.

3. ПОРЯДОК СТВОРЕННЯ КТЗІ

Для об'єктів електронно-обчислювальної техніки (ЕОТ), на яких циркулює інформація, що становить державну таємницю є обов'язковим створення та атестація КТЗІ, який має забезпечувати захист інформації з обмеженим доступом від витіку технічними каналами, а саме каналам побічних електромагнітних випромінювань та наведень.

Комплекс технічного захисту інформації — сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витіку інформації з обмеженим доступом технічними каналами на об'єктах інформаційної діяльності [16]. Створення та випробування КТЗІ здійснюється відповідно до положень НД ТЗІ 1.1-005-07, НД ТЗІ 1.6-003-04, НД ТЗІ 3.1-001-07, НД ТЗІ 3.3-001-07, НД ТЗІ 2.1-002-07 [16...20].

Для визначення необхідних заходів захисту інформації від витіку технічними каналами проводиться спеціальне дослідження персональної електронно-обчислювальної машини по каналах ПЕМВН, при якому визначаються можливі канали витіку інформації. За результатами спеціального дослідження приймається рішення про необхідність встановлення активних та/або пасивних засобів захисту. Після цього проводиться оцінка захищеності ІзОД від витіку технічними каналами на об'єкті ЕОТ (атестація комплексу

ТЗІ). Порядок виконання робіт та нормативне забезпечення питань створення КТЗІ на ОІД схематично відображено на рис. 4.

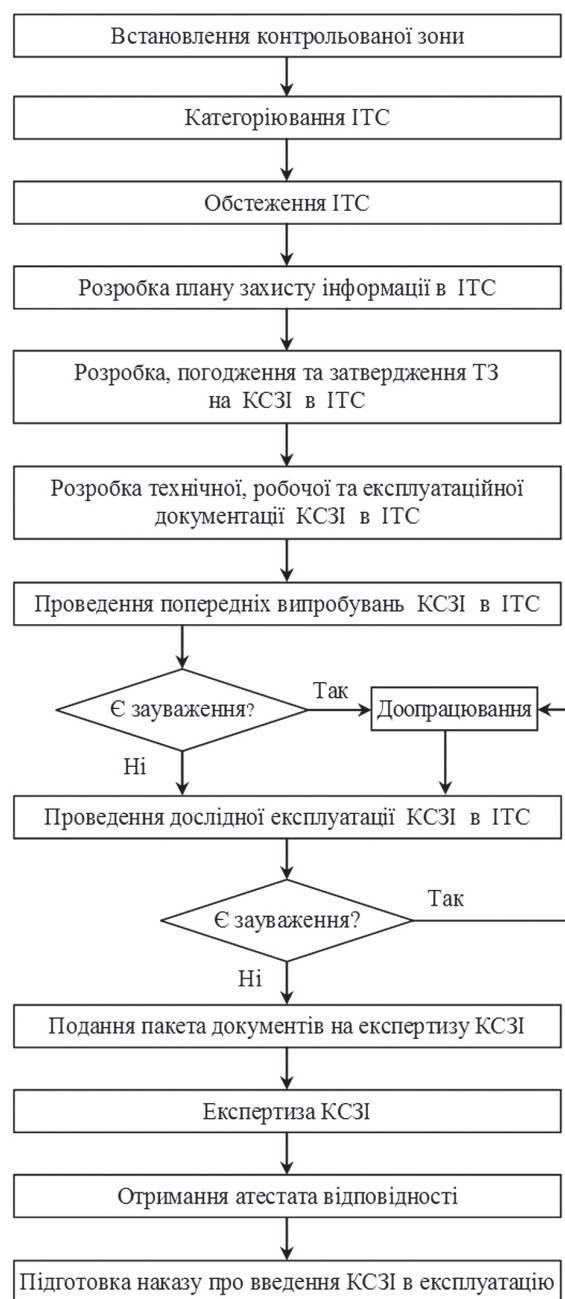


Рис. 3. Порядок створення КСЗІ в ІТС



Рис. 4. Порядок виконання робіт створення КТЗІ на ОІД

ВИСНОВКИ

На закінчення слід зазначити, що під час створення КСЗІ в ІТС необхідно дотримуватися певних методологічних принципів проведення досліджень, проектування, експлуатації і розвитку таких систем відповідно до вимог законодавства України. Порядок створення КСЗІ є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка є власністю держави.

Таким чином, у даній статті наведено порядок та етапи створення КСЗІ в ІТС і посилання на діючі нормативні документи, визначений обсяг і зміст робіт, етапності робіт, основні завдання та порядок виконання робіт кожного етапу та якими результатами вони повинні закінчуватися.

Література

- [1] *Про внесення змін до Закону України “Про інформацію”* № 2938-VI від 13.01.2011. — Відомості Верховної Ради України 2011, № 32, ст. 313. — (Серія видань “Законодавство України”).
- [2] *Про внесення змін до Закону України “Про Національну програму інформатизації”* № 2684-III від 13.09.2001. — Відомості Верховної Ради України 2002, № 1, ст. 3. — (Серія видань “Законодавство України”).
- [3] *Концепції технічного захисту інформації в Україні* № 1126 від 8.10.1997 р. — Із змінами, внесеними згідно з Постановою Кабінету Міністрів України № 938 від 07.09.2011. — (Серія видань “Законодавство України”).
- [4] *Закон України “Про захист персональних даних”* № 2297-VI від 01.06.2010. — Відомості Верховної Ради України 2010, № 34, ст. 481. — (Серія видань “Законодавство України”).
- [5] *Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”* № 80/94-ВР від 05.07.1994. — Відомості Верховної Ради України 1994, № 31, ст. 286. — (Серія видань “Законодавство України”).
- [6] *НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.* — Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99. — (Серія видань “Нормативний документ”).
- [7] *НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.* — Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.1999. — (Серія видань “Нормативний документ”).
- [8] *Про внесення змін до Закону України “Про захист інформації в автоматизованих системах”* № 2594-IV від 31.05.2005. — Відомості Верховної Ради України 2005, № 26, ст. 347. — (Серія видань “Законодавство України”).
- [9] *Місюра С.М. Варіант захисту мовної інформації на об'єктах інформаційної діяльності / С.М. Місюра, В.В. Овсянніков, І.Р. Мальцева // Збірник наукових праць ВІТІ НТУУ “КПІ”. — 2011. — № 2. — С. 84—93.*
- [10] *Хлапонін Ю.І. Порядок та особливості проведення державної експертизи комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Ю.І. Хлапонін // Збірник наукових праць ВІТІ НТУУ “КПІ” — 2011. — № 2 — С. 123—127.*
- [11] *Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Ю.В. Землянко, О.А. Замула, О.О. Ткач, Н.І. Литвинова, Я.А. Пересічанська // Прикладная радиоэлектроника: науч.-техн. журнал: ХНУРЕ, 2010. — Том 9. — № 3 — С. 460—469.*
- [12] *НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.* — Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. — (Серія видань “Нормативний документ”).
- [13] *ТПКО-95. Тимчасове положення про категоріювання об'єктів* № 35 від 10.07.95. — Затверджено наказом Державного комітету країни з питань державних секретів та технічного захисту інформації № 35 від 10.07.95. — (Серія видань “Тимчасове положення”).
- [14] *Положення про Державну експертизу в сфері технічного захисту інформації.* — Затверджено наказом Адміністрації ДССЗІ України № 93 від 16.05.07. — Офіційний вісник України. — 2007. — № 52, ст. 2153. — (Серія видань “Нормативний документ”).
- [15] *НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.* — Затверджено наказом Адміністрації ДССЗІ України № 65 від 12 березня 2011. — (Серія видань “Нормативний документ”).
- [16] *НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.* — Затверджено наказом Адміністрації ДССЗІ України № 232 від 12.12.2007. — (Серія видань “Нормативний документ”).
- [17] *НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.* — Затверджено наказом Адміністрації ДССЗІ України № 232 від 12.12.2007. — (Серія видань “Нормативний документ”).
- [18] *НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.* — Затверджено наказом Адміністрації ДССЗІ України № 232 від 12.12.2007. — (Серія видань “Нормативний документ”).
- [19] *НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.* — Затверджено наказом Адміністрації ДССЗІ України № 232 від 12.12.2007. — (Серія видань “Нормативний документ”).
- [20] *НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз*

для інформації. — Затверджено наказом ДСТСЗІ СБ України № 04 від 10.03.2004. — (Серія видань “Нормативний документ”).

Надійшла до редколегії 15.07.2014



Онацкий Олександр Віталійович, канд. техн. наук, старший викладач кафедри інформаційної безпеки та передачі даних Одеської національної академії зв'язку ім. О. С. Попова. Наукові інтереси: безпека інформаційних технологій, методологія створення комплексних систем захисту інформації.

УДК 004.056.55: 003.26

Методология создания комплексной системы защиты информации / Онацкий А.В. // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 350–356.

Рассматривается методология создания комплексной системы защиты информации согласно тре-

бованиям законодательства Украины. Приведен порядок и этапы создания комплексной системы защиты информации в информационно-телекоммуникационных системах.

Ключевые слова: комплексная система защиты информации, информация с ограниченным доступом, автоматизированная система, информационно-телекоммуникационная система.

Рис.: 4. Библиогр.: 20 назв.

UDK 004.056.55: 003.26

The methodology of creating the complex system of information protection / Onatskiy A.V. // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 350–356.

The methodology of creating the complex system of information protection according to the requirements of the legislation of Ukraine is considered. The order and stages of creating the complex system of information protection in information and telecommunication systems are given.

Keywords: complex system of information protection, information with limited access, automated system, information and telecommunication system.

Fig.: 4. Ref.: 20 items.

ІМІТАЦІЙНА МОДЕЛЬ ОЦІНКИ ЗАВАДОСТІЙКОСТІ КВАЗІКОГЕРЕНТНОЇ ДЕМОДУЛЯЦІЇ OFDM-СИГНАЛУ ПІД ЧАС ОБРОБКИ «В ЦІЛОМУ»

О.М. РОМА, О.М. БЕЛАС, Б.А. НИКОЛАЄНКО

У статті розглянуто оцінювання завадостійкості процедури квазікогерентної демодуляції OFDM-сигналу під час обробки сигналу «в цілому» на основі «групового» спостереження за допомогою імітаційного моделювання.

Ключові слова: квазікогерентна демодуляція, OFDM — Orthogonal Frequency Division Multiplexing, BPSK — Binary Phase-Shift Keying, завадостійкість, імітаційне моделювання.

ВСТУП

Сучасний рівень бойової готовності силових структур України та його подальше підвищення значно залежать від процесу удосконалення систем та зразків техніки зв'язку спеціального призначення.

В забезпеченні своєчасного, достовірного та прихованого управління важливе значення має радіозв'язок, альтернативи якого у ряді випадків може не бути.

Одним із ключових факторів, що впливають на якість радіозв'язку силових структур, є ненавмисні та навмисні завади.

Тому, в умовах апріорної невизначеності щодо умов ведення зв'язку, сигнально-завадової обстановки, **важливою і актуальною є задача** побудови високоефективних систем радіозв'язку, в яких забезпечується передача сигналів з допустимим рівнем адитивних спотворень.

Загальновідомо, що важливим показником ефективності, особливо для систем радіозв'язку спеціального призначення, є показник завадостійкості.

Проведений аналіз існуючих методів підвищення завадостійкості систем радіозв'язку спеціального призначення показав, що перспективним напрямком вирішення цього завдання при передачі сигналів багатопроменими каналами зв'язку є застосування методу ортогонального частотного розділення — мультиплексування (OFDM), сутність якого полягає в розділенні високошвидкісного потоку даних на множину паралельних низькошвидкісних підпотоків, кожний з яких модулюється своїм цифровим потоком [1–4]. Основними перевагами даного методу є стійкість до завмирань сигналу за умов багатопроменивості, висока частотна ефективність, а також можливість застосування різних схем модуляції окремо для кожної піднесівної частоти, що дозволяє адаптивно варіювати завадостійкість і швидкість передачі.

Характерним прикладом застосування OFDM-технологій в системах зв'язку силових структур є мобільний комплекс «МІК-МКС» фірми «Мікран», призначений для організації та швидкого розгортання цифрових радіорелейних ліній зв'язку, а також мереж широкосмугового бездротового доступу, побудованих за стандартом

802.16. Саме наявність даного стандарту дозволяє здійснювати прив'язку мобільних абонентів (у радіусі до 30 км) до базових станцій, які є основною компонентою опорної польової мережі зв'язку.

При цьому слід припустити, що за необхідністю забезпечення радіозв'язку з мобільними абонентами в складній сигнально-завадовій обстановці позиційність модуляції на піднесівних буде невеликою, до мінімальної включно.

При переході до методу модуляції мінімальної позиційності, з'являється можливість застосувати не квадратурну, як це має місце у стандарті 802.16, а квазікогерентну демодуляцію сигналів. А у цьому випадку в області низьких відношень сигнал/шум квазікогерентний демодулятор у порівнянні з некогерентним може надати вигрash у енергетиці сигналу до 2,5 дБ.

Тому, на першочергову увагу заслуговує, реалізація не квадратурної (як це має місце у стандарті 802.16xx), а квазікогерентної демодуляції OFDM-сигналів з ФМ-2 двійковою фазовою модуляцією.

1. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

За допомогою методів оптимальної нелінійної фільтрації дискретно-неперервних марківських процесів [5–7] та загальновідомої теорії [5–6] синтезовані деякі процедури квазікогерентної демодуляції OFDM-сигналу під час обробки «в цілому», на основі «групового» спостереження за усіма піднесівними частотами [8], а також виконано асимптотичну оцінку їх завадостійкості. Однак питання щодо підтвердження роботоздатності синтезованої у [8] процедури квазікогерентної демодуляції OFDM-сигналу під час обробки сигналу «в цілому» на основі «групового» спостереження залишається не вирішеним, оскільки такі методи аналізу в науковій літературі відсутні, а отримання точних математичних співвідношень для такого аналізу є складною задачею. Одним із шляхів ефективного вирішення цього питання є використання засобів імітаційного моделювання, зокрема — Matlab з пакетом розширення Simulink [9], яка для моделювання лінійних і нелінійних динамічних систем надає користувачу прості і зручні засоби,

в тому числі візуального об'єктно-орієнтованого програмування.

Зважаючи на вищесказане, для імітаційного моделювання демодулятора OFDM-сигналу під час обробки сигналу «в цілому» на основі «групового» спостереження використано версію Matlab R2013b з пакетом розширення Simulink.

Виходячи з актуальності питання та наявності невирішених задач, метою статті є розробка інструменту підтвердження роботоздатності синтезованої у [8] процедури квазікогерентної демодуляції OFDM-сигналу під час обробки сигналу «в цілому» на основі «групового» спостереження.

Постановка завдання дослідження на концептуальному рівні:

- підтвердження роботоздатності синтезованої процедури квазікогерентної демодуляції OFDM-сигналу під час обробки «в цілому» на основі «групового» спостереження;

- підтвердження результатів оцінювання завадостійкості квазікогерентного прийому сигналу із застосуванням процедури квазікогерентної демодуляції OFDM-сигналу під час обробки сигналу «в цілому» на основі «групового» спостереження.

Об'єктом моделювання є демодулятор OFDM-сигналу, що реалізує процедуру квазікогерентної демодуляції сигналу з ФМ-2 (BPSK).

Обмеження та припущення:

- вхідне спостереження є адитивною сумішшю корисного OFDM-сигналу з ФМ-2 та АБГШ. Обробка спостереження здійснюється в межах динамічного діапазону приймача;

- канал із постійними (повільно змінними) параметрами порівняно з тривалістю тактового інтервалу;

- початкові фази сигналу аналітично пов'язані;

- питання синхронізації опорного коливання по фазі та частоті, а також тактової синхронізації передавача та приймача уже вирішені;

- відсутнє явище зворотної роботи, яке характерно для всіх практичних способів формування опорного коливання в схемах прийому сигналів з фазовою маніпуляцією;

- у передавачі передбачена можливість штучного внесення неузгодженості за фазою опорного коливання передавача та приймача шляхом додавання до фази опорного коливання передавача постійного або повільно-змінного значення набігу фази. Параметри модулятора підібрані так, що частота несінного коливання в 64 рази вище бітової швидкості інформаційних символів, а частота дискретизації опорного коливання дорівнює $1/8$ періоду. Тобто частота дискретизації в 512 разів вища за бітову швидкість інформаційних символів. Ця ситуація відповідає випадку, коли в ході використання несінного коливання 2,4 ГГц, бітова швидкість передавача складає 37,5 Мбіт/с, що характерно для сучасних цифрових пристроїв.

Обмеження та припущення застосовані до тих процесів, які використовуються під час обробки сигналів, досить повно досліджені, мають відомі технічні рішення та практично реалізовані в приймальних радіозасобах.

2. ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Для дослідження властивостей, характеристик завадостійкості квазікогерентного прийому OFDM-сигналу, за допомогою пакета Simulink була розроблена «спрощена» імітаційна модель,

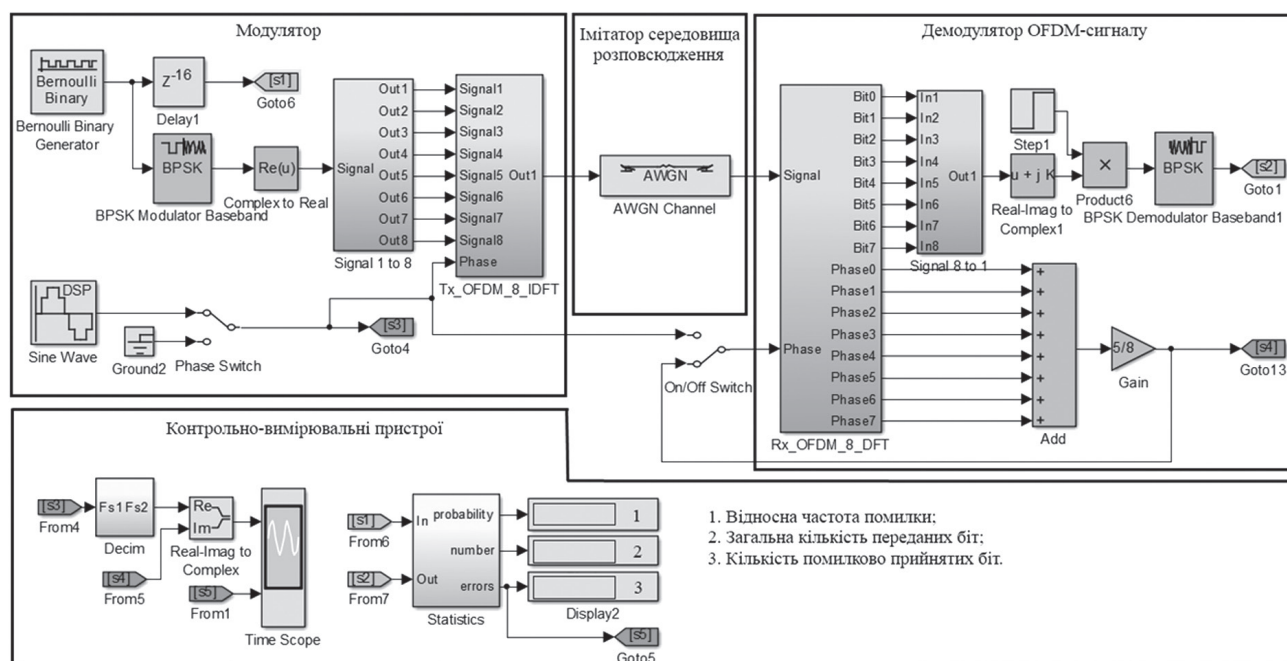


Рис. 1. Структурна схема імітаційної моделі квазікогерентного демодулятора OFDM-сигналу з ФМ-2 під час обробки «в цілому» на основі «групового» спостереження

Таблиця 1

Позначення, які застосовуються у структурній схемі імітаційної моделі квазікогерентного демодулятора OFDM-сигналу

Елемент	Функція	Призначення
Bernoulli Binary Generator	генератор псевдовипадкової послідовності Бернуллі	генерація випадкових двійкових чисел, використовуючи розподіл Бернуллі
BPSK Modulator Baseband	BPSK модулятор	модуляція методом двійкової фазової маніпуляції
Pulse Generator	генератор імпульсів	генерація послідовності імпульсів
Signal 1 to 8	послідовно-паралельний перетворювач	перетворення послідовного високошвидкісного потоку на множину паралельних низькошвидкісних підпотоків за кількістю піднесівних
Tx_OFDM_8_IDFT	формував OFDM-символів	формування радіоімпульсів, шляхом перемноження високо-частотних коливань кожної піднесівної на низькошвидкісні підпотоки
Rx_OFDM_8_DFT	приймач OFDM-символів	демодуляція OFDM-символів з корекцією початкової фази опорних коливань
Delay	затримка сигналу	затримка сигналу на заданий час
Triggered		буферизація сигналу затриманого на період
Complex to Real-Imap	елемент розділення «дійсної» та «уявної» частини	розділення «дійсної» та «уявної» частини сигналу
Sine Wave	генератор синусоїдального коливання	штучне внесення набігу фаз
Product	перемножувач	перемноження сигналів
Add	суматор	сумування сигналів
AWGN Chanel	канал з АБГШ	елемент імітації каналу розповсюдження сигналу з АБГШ
Trigonometric Function	гіперболічний тангенс	виведення результату щодо знаку імпульсу «+» або «-»
Discrete-Time Integrator	дискретний часовий інтегратор	накопичування сигналу впродовж інформаційного тактового інтервалу
Decim	елемент децимації	пониження частоти дискретизації
Gain	підсилювач	підсилення сигналу
Ground	заземлювач	відключення входу
Real-Imap to Complex	елемент об'єднання «дійсної» та «уявної» частини	об'єднання «дійсної» та «уявної» частини сигналу
Step	функція «одиночного стрибка»	включення демодулятора лише у момент початку демодуляції BPSK-сигналу, виключаючи його роботу по чистому шуму
On/off Switch	комутатор	включення / виключення каналу підлаштування фази
Phase Switch	комутатор	включення / виключення блоку внесення набігу фази в канал
OE2	управляючий елемент	формування сигналу фази неузгодженості між переданим та прийнятим сигналами
BPSK Demodulator Baseband	BPSK демодулятор	демодуляція методом двійкової фазової маніпуляції (ФМ-2)
Statistics	контрольно-вимірювальні пристрої	пристрої обчислення частоти помилки (probability), загальної кількості переданих біт (number) та кількості помилково прийнятих біт (errors)
Display	дисплей	відображення даних, що поступають із блоку Statistics
Time Scope	цифровий осцилограф	відображення сигналу в часовій області

яка передбачає роботу з 8-точковим OFDM-сигналом, та використовує BPSK-модуляцію. OFDM-сигнал містить лише 8 піднесівних, без зазначення їх призначення. Тобто присутні лише інформаційні складові сигналу (відсутні: циклічні префікси, пілот-сигнали, захисні інтервали та виключення центральної піднесівної), що не впливає на сам характер когерентного прийому.

Розглянемо компоненти блок-схеми імітаційної моделі.

Модулятор моделі вхідного спостереження формує OFDM-сигнал з BPSK модуляцію.

Сигнал створюється генератором псевдовипадкової послідовності Бернуллі. Перенесення спектра сформованого OFDM-сигналу на несівну частоту відбувається за допомогою високочастотного модулятора.

Для забезпечення імітації реальних умов розповсюдження радіохвиль використовується стандартний елемент (AWGN), який імітує канал з АБГШ та дає можливість встановлювати задане відношення сигнал/шум при введенні вхідних даних для моделювання.

Квазікогерентний демодулятор OFDM-сигналу з BPSK-модуляцією містить два канали: інформаційний та канал підлаштування фази.

Контрольно-вимірювальні пристрої в імітаційній моделі є пристрої обчислення частоти помилки, як оцінки середньої ймовірності помилки прийому інформаційного символу сигналу, а пристроями вимірювання – осцилографи, які відображають осцилограми в контрольних точках імітаційної моделі.

Модель містить обчислювач відповідної частоти помилки – *probability*, лічильник кількості переданих інформаційних біт – *number* та лічильник числа помилково переданих біт – *errors*.

Як показник ефективності використовується величина середньої частоти помилки прийому інформаційного символу сигналу $P_{\text{пом}}$, що визначається як відношення кількості помилково прийнятих інформаційних символів (біт) $N_{\text{пом}}$ до загальної кількості переданих символів сигналу $N_{\text{заг}}$ [10, 11]. На практиці, для достатньо великих $N_{\text{заг}}$ частота помилки прийому інформаційного символу визначається як: $P_{\text{пом}} = \lim_{N_{\text{заг}} \rightarrow \infty} N_{\text{пом}} / N_{\text{заг}}$

3. МОДЕЛЮВАННЯ

Наведемо частоту помилки $P_{\text{пом}}$ від різних значень відношення сигнал/шум ($P_c / P_{\text{ш}}$) для:

1. Оптимального когерентного приймача сигналів ФМ-2 за формулою [12]:

$$P_{\text{пом(фм)}} = 1 - F(\sqrt{2h^2}), \quad (1)$$

де $F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x \exp\left(-\frac{t^2}{2}\right) dt$ – функція Лапласа;

$h = \sqrt{\frac{E}{N_0}}$; $E = E_i = \int_0^T c_i^2(t) dt$, $i = 0, 1, \dots$ – енергія елемента сигналу; N_0 – одностороння спектральна щільність потужності білого шуму.

2. Оптимального некогерентного приймача сигналів ФМ-2 за формулою [12]:

$$P_{\text{пом(фм)}} = \frac{1}{2} e^{-h^2}. \quad (2)$$

3. Розробленого за допомогою імітаційної моделі квазікогерентного демодулятора OFDM-сигналу з ФМ-2 та ВФМ-2 під час обробки сигналу «в цілому» на основі «групового» спостереження з використання різної кількості піднесівних.

У табл. 2 та на рис. 2 отримані за допомогою вищенаведеної імітаційної моделі відношення частоти помилки $P_{\text{пом}}$ для різних видів прийому сигналів від значень сигнал/шум ($P_c / P_{\text{ш}}$).

Із рис. 2 видно, що застосування усіх піднесівних у OFDM-сигналі під час обробки «в цілому» на основі «групового» спостереження

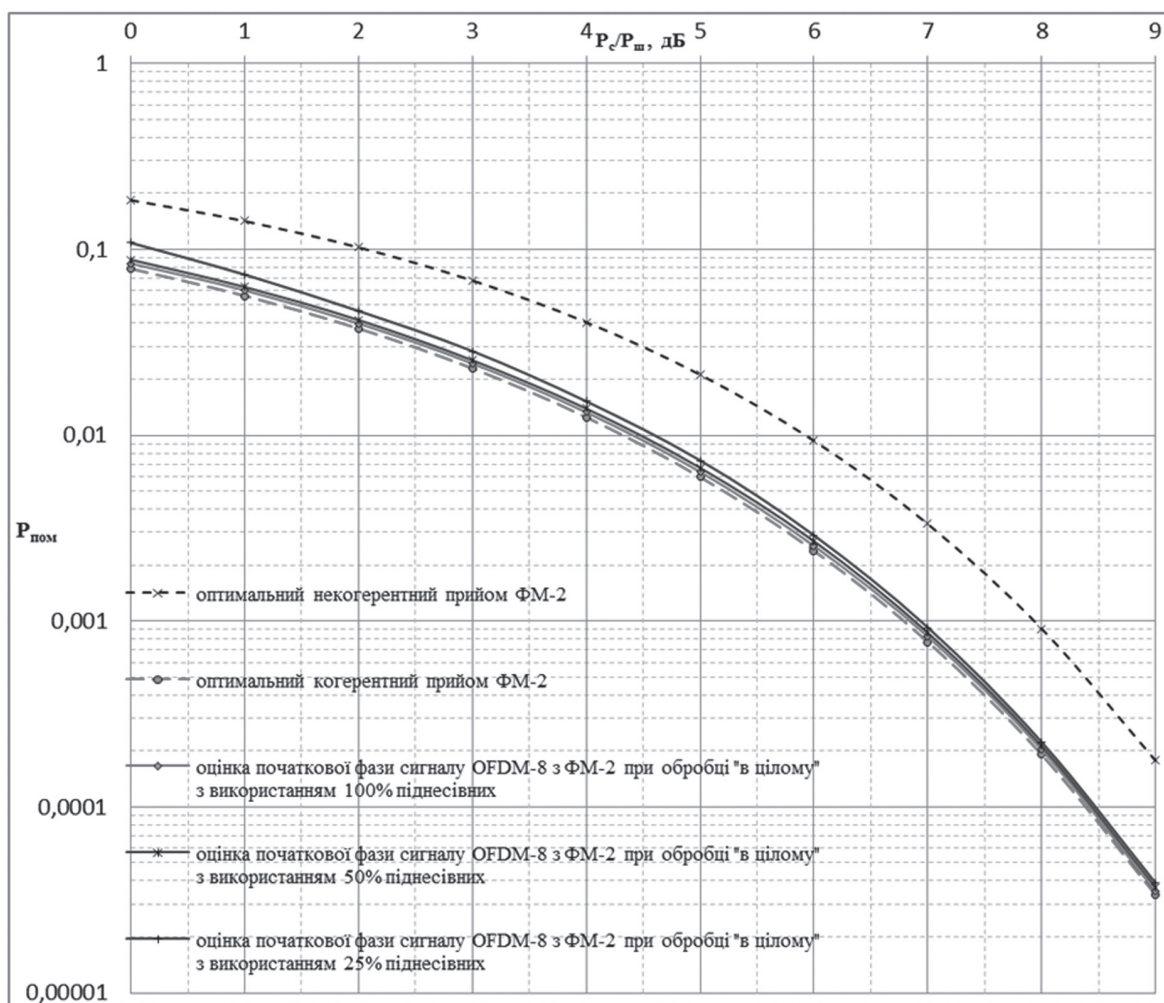


Рис. 2. Залежність частоти помилки $P_{\text{пом}}$ для різних видів прийому від значень сигнал/шум ($P_c / P_{\text{ш}}$)

Таблиця 2

Залежність відносної частоти помилки для різних значень відношення сигнал/шум

Сигнал/шум, $P_c/P_{ш}$ (дБ)	0	1	2	3	4	5	6	7	8	9
h^2 , (рази)	1	1,25892	1,58489	1,99526	2,51188	3,16227	3,98107	5,01187	6,30957	7,94328
К-ть випробувань (n)	300000	300000	300000	300000	300000	400000	400000	400000	500000	1000000
Опт. ког. прм. ФМ-2	0,07865	0,05628	0,0375061	0,022878	0,012501	0,005954	0,002388	0,000773	0,0001909	0,000034
Опт. нек. прм ФМ-2	0,18394	0,14197	0,1024848	0,067989	0,040558	0,021165	0,009333	0,003329	0,000909	0,000177
OFDM-8 з 100% піднес.	0,08398	0,06024	0,03995	0,02431	0,01329	0,00635	0,002538	0,000825	0,000203	0,000035
OFDM-8 з 50% піднес.	0,08795	0,06273	0,04167	0,0253	0,01391	0,006678	0,00269	0,000865	0,000212	0,000037
OFDM-8 з 25% піднес.	0,1085	0,0732	0,04664	0,02835	0,01522	0,00732	0,002893	0,000923	0,000223	0,000039

дозволяє якомога ближче наблизитися до оптимального когерентного прийому.

Для визначення енергетичного програшу при переході від оптимального когерентного прийому до оптимального некогерентного та від когерентного до синтезованого за допомогою імітаційного моделювання квазікогерентного прийому OFDM-сигналу з ФМ-2 в ході застосування різної кількості піднесівних, використовуємо наступні значення (табл. 3), що були розраховані з рис. 2.

Таблиця 3

Залежність енергетичних витрат відносно оптимального когерентного прийому сигналів ФМ-2 при різних видах прийому

Частота помилки ($P_{пом}$)	0,08	0,01	0,001	0,0001
Опт. некогерентний прм.	2,62	1,62	1,13	0,89
OFDM-8 з 100 % піднесівних	0,79	0,31	0,16	0,1
OFDM-8 з 50 % піднесівних	0,41	0,17	0,1	0,07
OFDM-8 з 25 % піднесівних	0,31	0,1	0,06	0,03

Із рис. 3 визначимо енергетичний виграш (табл. 4), при переході від некогерентного до квазікогерентного приймання OFDM-сигналу з ФМ-2 під час обробки «в цілому» для різної кількості піднесівних (рис. 4).

Таблиця 4

Енергетичні виграші відносно оптимального некогерентного прийому для різних видів демодуляцій з використанням ФМ-2

Частота помилки ($P_{пом}$)	0,08	0,01	0,001	0,0001
Опт. ког. прм. з ФМ-2	2,62	1,62	1,13	0,89
Виграш OFDM-8 з 100 % піднесівних	1,83	1,31	0,97	0,79
Виграш OFDM-8 з 50 % піднесівних	2,21	1,45	1,03	0,82
Виграш OFDM-8 з 25 % піднесівних	2,31	1,52	1,07	0,86

ВИСНОВКИ

На основі імітаційного моделювання квазікогерентного демодулятора OFDM-сигналу під

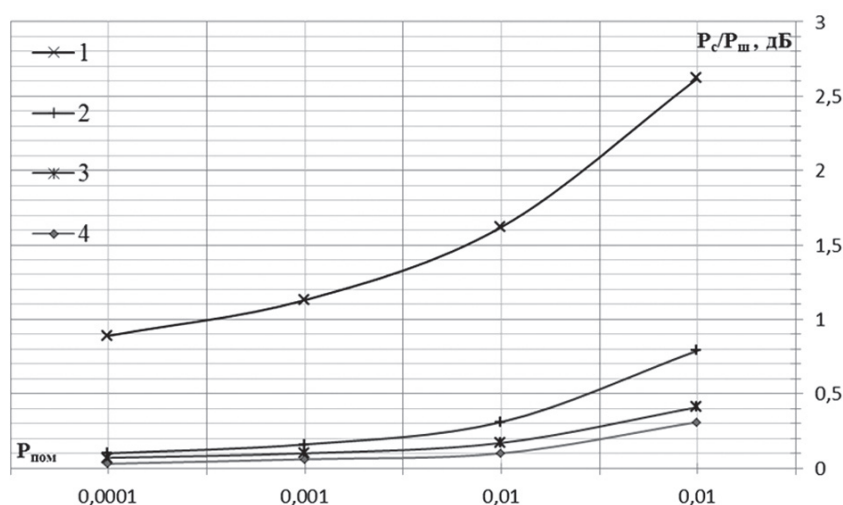


Рис. 3. Залежність енергетичних витрат відносно оптимального когерентного прийому сигналів ФМ-2 при:
1 — оптимальному некогерентному прийомі; 2 — квазікогерентному прийомі сигналу OFDM-8 з оцінкою початкової фази під час обробки «в цілому» з використанням 25 % піднесівних; 3 — квазікогерентному прийомі сигналу OFDM-8 з оцінкою початкової фази під час обробки «в цілому» з використанням 50 % піднесівних; 4 — квазікогерентному прийомі сигналу OFDM-8 з оцінкою початкової фази під час обробки «в цілому» з використанням 100 % піднесівних

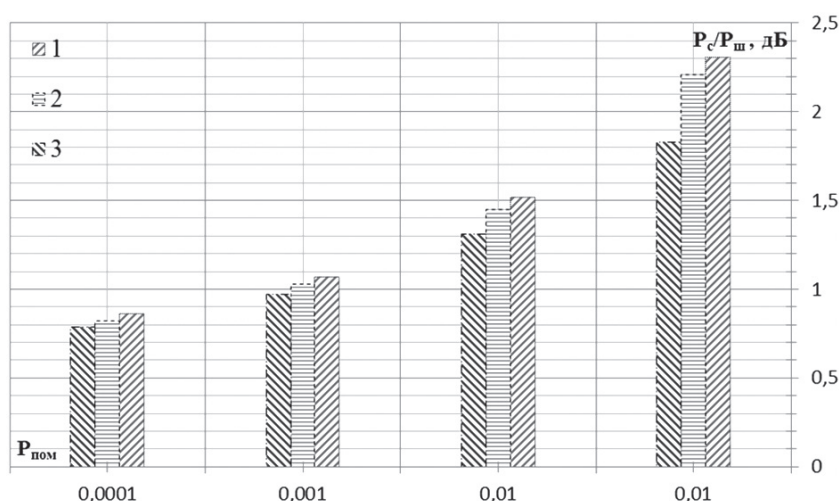


Рис. 4. Энергетичні виграти при переході від некогерентної до квазікогерентної демодуляції OFDM-сигналів з ФМ-2 під час обробки «в цілому» (для різної кількості піднесівних): 1 – квазікогерентний прийом сигналу OFDM-8 з оцінкою початкової фази під час обробки «в цілому» з використанням 100 % піднесівних; 2 – квазікогерентний прийом сигналу OFDM-8 з оцінкою початкової фази під час обробки «в цілому» з використанням 50 % піднесівних; 3 – квазікогерентний прийом сигналу OFDM-8 з оцінкою початкової фази під час обробки «в цілому» з використанням 25 % піднесівних

час обробки «в цілому» здійснено оцінку завадостійкості.

Встановлено, що перехід від квадратурної до квазікогерентної демодуляції OFDM-сигналу в ході використання ФМ-2 дозволяє підвищити показник завадостійкості систем радіозв'язку спеціального призначення на 0,8 – 2,3 дБ (1,20 – 1,69 рази).

Результат вирішення поставленого завдання можна рекомендувати до використання у перспективній технології LTE Advanced та у засобах зв'язку силових структур.

Література

- [1] Современные беспроводные сети: состояние и перспективы развития И.А. Гепко, В.Ф. Олейник, Ю.Д. Чайка, А.В. Бондаренко – Киев: «ЕКМО». – 2009. – 671 с.
- [2] Orthogonal Frequency Division Multiplexing (OFDM) [Електронний ресурс] // Режим доступу: http://www.comlab.hut.fi/opetus/311/ofdm_mod.pdf Дата доступу: – квітень 2012. – Назва з екрану.
- [3] Будущее за технологией LTE [Електронний ресурс] // Режим доступу: <http://www.nokiaamo.ru/main/471-budushhee-za-technologie-lte.html>. Дата доступу: – лютий 2011. – Назва з екрану.
- [4] Почему в WiMax и LTE используют OFDM [Електронний ресурс] // Режим доступу: <http://habrahabr.ru/blogs/wireless/129101/> – Дата доступу: – лютий 2011. – Назва з екрану.
- [5] Тихонов В.И. Статистический анализ и синтез радиотехнических устройств и систем: учеб. пособие для вузов / В.И. Тихонов. – М.: Радио и связь. – 1991. – 608 с.
- [6] Тихонов В.И. Нелинейная фильтрация и квазикогерентный прием сигналов. / В.И. Тихонов, Н.К. Кульман. – Сов. радио, 1975. – 704 с.
- [7] Дьяконов В.П. Matlab 6.5 SP1/7 + Simulink 5/6. Основы применения. Серия «Библиотека профессионала». – М.: СОЛОН-Пресс, 2005. – 800 с.

[8] Декл. пат. на кор. мод. України 88964. Пристрій фільтрації початкових фаз складових OFDM-сигналу при обробці «в цілому»; H04B1/00 / Б.А. Гиндич, В.Ф. Єрохін. – № u 2013 11857; Заявл. 08.10.2013; Опубл. 10.04.2014, Бюл. № 7. – 3 с.

[9] Волков Е. А. Численные методы : учебное пособие для вузов / Е. А. Волков. – М.: Наука. Главная редакция физико-математической литературы, 1987. – 248 с.

[10] Королюк В.С. Справочник по теории вероятности и математической статистике / В. С. Королюк, Н. И. Портенко, А. В. Скороход, А. Ф. Турбин. – [изд. Второе]. – М.: Наука, 1985. – 640 с.

[11] Гмурман В.Е. Теория вероятности и математическая статистика: учебное пособие для вузов / В.Е. Гмурман. – 9-е изд., стер. – М.: Высш. шк., 2003. – 479 с.: ил.

[12] Коржик В.И. Расчет помехоустойчивости систем передачи дискретных сообщений: Справочник / В.И. Коржик, Л.М. Финк, К.Н. Шелкунов: Под ред. Л.М. Финка. – М.: Радио и связь, 1981. – 232 с.

Надійшла до редколегії 5.08.2014



Рома Олександр Миколайович, доктор технічних наук, професор спеціальної кафедри № 3 застосування засобів спеціальних телекомунікаційних систем Інституту спеціального зв'язку та захисту інформації. Наукові інтереси: телекомунікації.



Белас Олег Миколайович, доктор технічних наук, професор спеціальної кафедри № 3 застосування засобів спеціальних телекомунікаційних систем Інституту спеціального зв'язку та захисту інформації. Наукові інтереси: телекомунікації.



Ніколаєнко Богдан Анатолійович, аспірант науково-організаційного відділу науково-дослідного центру Інституту спеціального зв'язку та захисту інформації. Наукові інтереси: технології 4-го покоління зв'язку LTE – Long Term Evolution, демодуляція складних сигналів типу OFDM – Orthogonal Frequency Division Multiplexing, імітаційне моделювання вищезазначених процесів.

УДК 621.396.1

Имитационная модель оценки помехоустойчивости квазікогерентной демодуляции OFDM-сигнала при обработке «в целом» / А.Н. Рома, О.Н. Белас, Б.А. Николаенко // Прикладная радиоэлектроника: научно-техн. журнал. — 2014. — Том 13. — № 3. — С. 357–363.

В статье была рассмотрена оценка помехоустойчивости процедуры квазікогерентной демодуляции OFDM-сигнала при обработке сигнала «в целом» на основе «группового» наблюдения с помощью имитационного моделирования.

Ключевые слова: квазікогерентная демодуляция, OFDM – ортогональное частотное разделение и мультиплексирование, BPSK – двоичная фазовая манипуляция, помехоустойчивость, имитационное моделирование.

Табл.: 04. Ил.: 04. Библиогр.: 12 назв.

UDC 621.396.1

Simulation model for evaluating noise immunity of OFDM-signal quasicohherent demodulation when processing «in general» / O.M. Roma, O.M. Belas, B.A. Nikolaienko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 357–363.

The paper deals with evaluation of noise immunity of the procedures OFDM-signal quasicohherent demodulation in the signal processing «in general» based on «group» supervision by means of simulation modelling.

Keywords: quasicohherent demodulation, OFDM – Orthogonal Frequency Division Multiplexing, BPSK – Binary Phase-Shift Keying, noise immunity, simulation modelling.

Tab.: 04. Fig.: 04. Ref.: 12 items.



**АЛМАЗОВ
ВЛАДИСЛАВ
БОРИСОВИЧ**
(11.10.1932–04.10.2014)

Ушел из жизни замечательный человек, выдающийся специалист в области радиолокации, организатор науки, педагог и общественный деятель, доктор технических наук, профессор, Заслуженный деятель науки Украины, начальник кафедры радиолокации Вирта ПВО им. Л.А. Говорова, полковник, создатель и первый президент Академии наук прикладной радиоэлектроники **Алмазов Владислав Борисович**.

Вся сознательная жизнь В.Б. Алмазова связана с военной наукой. Еще слушателем Академии он участвовал в создании уникального для того времени фильтра сжатия, решавшего важные задачи радиолокации. После окончания Академии с золотой медалью защищены кандидатская (1965 г.) и докторская (1970 г.) диссертации, создано новое направление в радиолокации, изданы 6 монографий и 5 учебников, написано свыше 350 статей и получено 49 авторских свидетельств на изобретения, подготовлены кандидаты и доктора наук, создана и до сих пор успешно работает Академия наук прикладной радиоэлектроники.

Коллеги и ученики, прошедшие школу жизни и науки под его руководством, тысячи слушателей и курсантов, прослушавших его блестящие лекции и семинары, навсегда сохраняют светлую память об Учителе и друге Владиславе Борисовиче АЛМАЗОВЕ.

Президиум АН ПРЭ

ПРИКЛАДНАЯ РАДИОЭЛЕКТРОНИКА

Научно-технический журнал

Ответственный секретарь

Е. Б. Исаева

Корректор

Б. П. Косиковская

Перевод на английский язык

К. Т. Умяров

Компьютерный дизайн и верстка

Е. Б. Исаева

Рекомендовано засіданням Бюро Президії Академії наук прикладної радіоелектроніки
(протокол № 3 від 25.09.2014 р.).

Рекомендовано Вченою радою Харківського національного університету радіоелектроніки
(протокол № 37 від 26.09.2014 р.).

Свідоцтво про державну реєстрацію КВ № 6037 від 09.04.2002 р.

Журнал включений до списку фахових видань ВАК України
з технічних наук
(постанова президії ВАК України № 1-05/2 від 10.03.2010),
з фізико-математичних наук (фізика)
(постанова президії ВАК України № 1-05/5 від 1.07.2010)

Підписано до друку 30.09.2014. Формат 60 × 84 ¹/₈.
Папір офсет. Друк офсет. Умов.-друк. арк. 21,16. Облік.-вид. арк. 21,0.
Тираж 300 прим. Ціна договірна.

Віддруковано в ТОВ «ДРУКАРНЯ МАДРИД»
61024, м. Харків, вул. Ольмінського, 11. Тел.: (057) 756-53-25
www.madrid.in.ua, e-mail: info@madrid.in.ua