СОДЕРЖАНИЕ

CONTENTS

ШАНОВНІ ЧИТАЧІ!

Випуск журналу є тематичним та присвячений розгляду ряду проблемних питань теорії та практики забезпечення безпеки інформації в інформаційних та інформаційно-телекомунікаційних системах. Значна частина статей є замовними. Зважаючи на актуальність, в журналі розміщені статті по таким трьом напрямам: методи та засоби аналізу та синтезу блокових симетричних шифрів; методи, механізми та протоколи криптографічного захисту; методи і засоби аналізу та оцінки безпеки інформації.

Перший розділ містить статті, що присвячені вирішенню проблемних питань оцінки криптографічної стійкості блокових симетричних шифрів (БСШ). Ряд статей пов'язані з розвитком нового концептуального підходу, що ґрунтується на дослідженнях криптографічної стійкості на зменшених версіях БСШ, причому вони розглядаються як перетворення підстановки. З використанням такого підходу оцінюються показники стійкості до атак диференційного та лінійного криптоаналізу. Показується, що лінійні властивості перетворень шифрування БСШ є проявом властивостей випадкових підстановок. Практична реалізація результатів зводиться до застосування теоретичних результатів для аналізу претендентів на національний стандарт БСШ. В цілому сукупність результатів та оцінок, що поміщені в першому розділі, дозволяють розробити та застосовувати науково обґрунтовані методики аналізу та порівняння існуючих та перспективних БСШ.

В другому розділі представлені статті, що пов'язані з проблемними питаннями та розвитком асиметричної криптографії. З теоретичної точки зору важливими є результати досліджень відносно застосування кривих Гурвиця з метою виконання універсального гешування. Також важливими є результати, що направлені на підвищення швидкодії асиметричних крипто перетворень. Тут є декілька напрямів підвищення швидкодії. Дещо нетрадиційним є застосування розпаралелювання, це скоріше всього один із важливих підходів до вирішення вказаної задачі. Для вирішення цих задач необхідно визначити базові операції для усіх алгоритмів, вибрати методи розпаралелювання та реалізувати їх для багатоядерних процесорів. Уже традиційними є дослідження, що пов'язані з асиметричними крипто перетвореннями зі спарюванням точок еліптичних кривих. Також практичний інтерес мають статті, що присвячені практичним додаткам криптографії в банківській сфері, міжнародній системі електронних цифрових паспортів, електронній автентифікації, стану стандартизації тощо.

Третій розділ містить результати досліджень, що пов'язані з оцінкою та аналізом безпеки інформації. Необхідно відмітити статтю, що посвячена онтологічного аналізу предметної області гарантій інформаційної безпеки. Підхід, що пропонується для оцінки рівня гарантій інформаційної безпеки, ґрунтується на функціональному моделюванні процесів оцінювання та введенні лінгвістичних змінних. З практичної точки зору є важливими результати, що пов'язані з аналізом та порівнянням систем оцінки показників безпеки інформації, розглядаючи таксономії показників безпеки інформації можна визначити їхні головні властивості, переваги та недоліки. Також в третьому розділі представлені статті, що пов'язані з вирішенням задач технічного захисту інформації, створення комплексних систем захисту інформації, стеганографії тощо.

Надіємось, що опубліковані в журналі статті будуть послуговувати подальшому розвитку та удосконаленню системи захисту інформації в Україні, вдосконаленні навчального процесу.

З повагою до читачів

Ректор ХНУРЕ

Бондаренко М.Ф.

Завідувач кафедри безпеки інформаційних технологій ХНУРЕ

Горбенко І.Д.

МЕТОДЫ И СРЕДСТВА АНАЛИЗА И СИНТЕЗА БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

УДК 681.3.06

НОВАЯ ИДЕОЛОГИЯ ОЦЕНКИ СТОЙКОСТИ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

И.Д. ГОРБЕНКО, В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, Р.В. ОЛЕЙНИКОВ

Предлагается подход к оценке безопасности блочных шифров, ориентированный, с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа показателей уменьшенных их версий, а с другой, на использование уточнённой в последнее время на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, концепции (новой идеологии) определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа.

Ключевые слова: дифференциальный и линейный криптоанализ, показатели стойкости к атакам линейного и дифференциального криптоанализа, свойства случайных подстановок и шифрующих преобразований.

ВВЕДЕНИЕ

Последнее время появился ряд публикаций, в которых обсуждаются подходы к построению (получению) оценок доказуемой безопасности блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа [1-5 и др.].

Мы здесь кратко напомним результаты некоторых известных работ, относящихся к оценкам стойкости БСШ к атакам дифференциального и линейного криптоанализа.

В [1] изучается подстановочно-перестановочная схема (SPN), на которой строится AES. Вводится AES* – SPN шифр, идентичный AES за исключением того, что фиксированные S-блоки заменены случайными и независимыми перестановками. Доказывается, что эта конструкция сопротивляется линейному и дифференциальному криптоанализу начиная с 4-х внутренних циклов, несмотря на огромный совокупный эффект многопутевых характеристик, которые порождены симметрией AES. Показывается, что дифференциальная и линейная вероятности (*DP* и *LP* условия) обе стремятся к значению $1/(2^{128}-1)$ очень быстро с ростом числа циклов. Подчеркивается, что результат подтверждает предположение исследователей Keliher, Meijer и Tavares.

В [2] Keliher и др. представили новый метод определения верхней границы максимума средней вероятности линейного корпуса (*MALHP*) для SPN шифров – значения, которое позволяет, как считают они, обосновать утверждение о доказуемой безопасности к атакам линейного криптоанализа. Применение этого метода к Rijndael-ю (AES) с 7-ю и более циклами обеспечивает верхнюю границу $UB = 2^{-75}$, соответствующая нижняя граница сложности данных есть $\frac{32}{UB} = 2^{80}$ (для 96,7% отношения успеха).

В [3] улучшается эта верхняя граница для Rijndael-я на основе рассмотрения значений распределения линейных вероятностей для (уникального) S-блока Rijndael-я. Получена верхняя граница для *MALHP*. Для Rijndael-я с 9 циклами дается значение 2^{-92}, соответствующее нижней границе сложности данных 2^{97} (снова для 96,7% отношения успеха). (После проведения 43% вычислений, авторы полагают, что полученное значение уже стабилизировалось).

В [4] определены аналитические верхние оценки средних вероятностей дифференциальных и линейных характеристик блочных шифров, построенных по схеме шифра «Калина-128». В частности, в работе приводятся такие оценки для отмеченных показателей: $EDP \le 2^{-130}$, $ELP \le 2^{-130}$. Авторы относят эти оценки к показателям практической стойкости шифра.

В [5] расширяется теорема Хонга и др., которая дает верхние границы для максимумов средних вероятностей дифференциалов и линейных корпусов (*MADP* и *MALHP*), на SPN блоковых шифров с оптимальными или квазиоптимальными диффузионными слоями для случая вложенных SPN (NSPN) структур. Применение расширенной теоремы для двух NSPN шифров Hierocrypt-3 со 128-битными блоками и Hierocrypt-L1 с 64-битными блоками позволило авторам получить оценки для *MADP* и *MALHP* для 2-х циклового Hierocrypt-3 приводящие к границе 2^{-96} и для Hierocrypt-L1 с двумя циклами к границе 2^{-48}. Расширенная теорема была применена также для AES и позволила утановить, что *MADP* и *MALHP* для 4-х цикловой уменьшенной модели ограничены значением 2^{-96}. Этот результат, отмечают авторы, превосходит лучший предыдущий результат 2^{-92} для 10-ти циклов Keliher-а и др. Результат опять связывается с дифференциальными

и линейными свойствами входящих в шифр S-блоков и числом ветвлений.

Можно привести и много других работ, посвященных оценке показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа.

Первый вывод, который можно сделать из приведенных результатов, состоит в том, что оценки соответствующих показателей отличаются в значительных пределах. Второй вывод состоит в том, что результирующие показатели стойкости шифров практически во всех работах связываются с соответствующими криптографическими показателями, входящих в шифры S блоковых конструкций.

Следует заметить, что сам термин доказуемая безопасность уже давно введен в криптографии. Когда говорят о доказуемой Безопасности ("Provable" Security), отмечается в документе [6], то обычно имеют в виду одно из двух.

Во-первых, если можно показать, что взлом шифра является таким же трудным, как решение некоторой хорошо известной трудной проблемы (например, дискретного логарифмирования или факторизации), то шифр считается доказуемо безопасным. Здесь, конечно, есть рассогласование (ввод в заблуждение), так как трудная проблема, к которой сводятся рассуждения, обычно не доказуемо трудная. Это подход имеет отношение к фундаментальному открытому вопросу в компьютерной науке, являются ли трудные проблемы P или NP полными задачами? Фактически, доказуемая безопасность требует доказательства, что $P \neq NP$, и существования односторонних функций, которые в одну ″сторону″ являются трудными для вычисления *в среднем* (в вероятностном смысле), но в другую могут быть решены быстро при наличии некоторой экстра информации. Заметим, что меры сложности здесь *асимптотические* – уровень сложности оценивается через входной размер в битах на бесконечности. Отмечается, что стратегия отнесения задач оценки стойкости криптосистем к тяжелым проблемам очень полезна для практического анализа шифров, хотя эту модель изначально относили к криптосистемам с открытым ключом.

Во-вторых, шифр может показывать доказуемую безопасность против целого набора атак. Тем не менее, это, очевидно, не означает, что шифр безопасный против всех атак.

Начиная с работы K. Нюберг и Л. Кнудсена [7] для обозначения свойства блочного шифра иметь достаточно малую дифференциальную вероятность, тоже начали использовать понятие доказуемой безопасности (″Provable security″) к атакам дифференциального криптоанализа. В последующих публикациях [8 и др.] аналогичное понятие появилось для определения стойкости шифров и к атакам линейного криптоанализа.

На наш взгляд, однако, более адекватным для блочных шифров следует считать понятие практической безопасности (Practical Security) [6]. В этой модели блочный шифр считается вычислительно безопасным, если наилучшая из известных атак требует слишком много ресурсов из допустимого запаса. Это очень практичная модель, так как всегда можно протестировать шифр на устойчивость к различным известным атакам, изучая его слабости, а затем дать оценку устойчивости шифра к таким атакам с точки зрения необходимых ресурсов времени/пространства. Она позволяет получить большинство ответов, и большинство анализов, встречающихся в литературе, в том числе и на прошедших конкурсах AES и NESSIE было именно этого типа. Конечно, и в этом случае полученные результаты опять ничего не говорят об уровне безопасности по отношению ко все еще неизвестным атакам. Заключая этот небольшой анализ подходов к оценке безопасности шифров, можно отметить, что их авторы, по-видимому, под доказуемой безопасностью имели в виду то, что полученный ими результат можно считать надежно обоснованным. В этой редакции с ними можно согласиться.

В этой работе мы хотим высказать свою точку зрения по вопросу оценки безопасности блочных шифров, концептуально отличающуюся от известных, хотя в конечном итоге речь опять будет идти об определении максимальных значений полных дифференциалов и линейных корпусов (оболочек) БСШ.

Прежде всего, хотелось бы отметить, что все существующие подходы к оценке показателей стойкости БСШ опираются скорее на интуитивные соображения, подкрепленные результатами анализа под определенным углом зрения (субъективного) уменьшенных по числу циклов или упрощенных версий рассматриваемых БСШ. И это многим исследователям представляется вполне оправданным, так как полный анализ современного шифра при реальной длине битового размера входа является сегодня невыполнимой задачей. Собственно говоря, разработчики шифров и идут по пути увеличения размеров битового входа именно для того, чтобы сделать, по крайней мере, задачу полного перебора ключей или текстов не реализуемой в обозримом будущем. Поэтому многие подходы к оценке показателей стойкости больших шифров строятся скорее на основе накопленного опыта и некоторых соображений и оценок, позволяющих получить аргументы и данные для подтверждения предполагаемых высоких показателей стойкости предлагаемых решений. По этому пути пошли и разработчики шифра Rijendael. Они действительно предложили достаточно прозрачную для понимания и анализа конструкцию шифрующего преобразования, строящуюся на реализации популярной теперь стратегии широкого следа и допускающую достаточно убедительное прогнозирование ожидаемых показателей стойкости.

Конечно же, стратегия широкого следа не является открытием или новым словом в криптографии. Она по существу является реализацией классической стратегии перемешивания и перепутывания, обоснованной еще в работе К. Шеннона. Более того, общую идею практической реализации этой стратегии для SPN шифров уже давно (в 1973 году) продемонстрировал в своей работе [9] Х. Фейстель, своеобразно реализовавший ее затем и в шифре DES. Тем не менее, нужно отдать должное разработчикам Rijendael-я – их линейное преобразование оказалось существенно более эффективным (судя по данным экспериментов почти в два раза) по сравнению с простым (регулярным) перемешиванием (переключением) выходов и входов между слоями преобразований, как это сделано в решении Х. Фейстеля. Стремясь реализовать максимально возможные показатели преобразования по стойкости, они постарались использовать в своей конструкции и S-блоки с предельными дифференциальными и линейными показателями, даже допустив регулярность (алгебраичность) в построении нелинейных преобразований. В целом же простота и прозрачность их конструкции обеспечивается в основном за счет того, что они фактически повторили классическую схему SPN шифра, описанного Х. Фейстелем.

Интуиция их, правда, подвела при выборе конструкции S блоков. Они посчитали, что показатели S блоков оказывают решающее влияние на итоговые показатели стойкости шифра. На самом деле, как мы покажем, это не так и, соответственно, действительные показатели стойкости к атакам дифференциального и линейного криптоанализа будут несколько иными.

Излагаемые далее соображения и результаты строятся исходя из развитого нами нового подхода в теории и методах криптоанализа [10], ориентированного, с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа уменьшенных их версий, а с другой, – уточнённой в последнее время на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, концепции (новой идеологии) определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа.

Итак, для преодоления трудностей анализа полномасштабных моделей (алгоритмов) шифрования мы пошли по пути разработки и исследования уменьшенных моделей прототипов, для которых имеющихся вычислительных ресурсов оказывается уже вполне достаточно [10]. Наши проработки показывают, что большое число хорошо известных алгоритмов шифрования допускают масштабирование. Удается построить уменьшенные модели, которые сохраняют все свойства своих прототипов и позволяют решить многие задачи анализа и сравнения по показателям стойкости соответствующих больших версий.

Самый главный и неожиданный результат изучения уменьшенных моделей состоит в том, что общепринятая точка зрения, разрабатываемая во многих работах и состоящая в том, что линейные и дифференциальные свойства шифров непосредственно связаны со свойствами S-блоков, используемых при их построении, оказалась не верной или не совсем верной. На самом деле результирующие (т.е. получающиеся при использовании полного набора цикловых преобразований) показатели стойкости шифров определяются для большого числа вариантов выбора S блоков практически только размером битового входа в шифр.

Второй важный вывод, следующий из выполненных исследований, сводится к тому, что показатели стойкости больших (полных реализаций) шифров к атакам дифференциального и линейного криптоанализа (таких, как Rijndael и многих других известных шифров, а также шифров Лабиринт, Калина, Мухомор, ADE [11,12,13,14], представленных на украинский конкурс по выбору национального стандарта шифрования), могут быть получены расчетным путем.

В этой работе мы представляем некоторые из результатов проведенных исследований в развиваемом направлении и их интерпретацию в теоретическом и практическом понимании с наших позиций.

1. ПОНЯТИЙНЫЙ АППАРАТ ЛИНЕЙНОГО И ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА

Напомним кратко основной понятийный аппарат линейного и дифференциального криптоанализа. Следуя работе [14], введем ряд определений.

Определение 1 (Дифференциальная и Линейная вероятность)**:** *Дифференциальная вероятность* DP^f *и линейная вероятность* LP^f *соответственно для ключезависимой функции* f *с* n*-битным входом* x *и* n*-битным выходом* y, $x, y \in GF(2)^n$ *есть*

$$DP^f(\Delta x \to \Delta y) = \frac{\#\{x \in GF(2)^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n}, \quad (1)$$

$$LP^f(\Gamma y \to \Gamma x) = \left(\frac{\#\{x \in GF(2)^n \mid x \cdot \Gamma x = f(x) \cdot \Gamma y\}}{2^{n-1}} - 1\right)^2, \quad (2)$$

где Δx *и* Δy *являются входным и выходным различием (разностью), а* Γx *и* Γy *входной и выходной масками;* $x\,\Gamma x$ *обозначает результат побитного произведения* x *и* Γx.

Определение 2 ($DP^f_{\max}$ и $DL^f_{\max}$)**:** *Максимальное значение дифференциальной и линейной вероятности для ключезависимой функции* f *определяется соответственно как*

$$DP^f_{\max} = \max_{\Delta x \neq 0,\ \Delta y} DP^f(\Delta x \to \Delta y), \quad (3)$$

$$DL^f_{\max} = \max_{x,\ y \neq 0} DL^f(\ y \to\ x). \quad (4)$$

В общем случае, ключезависимая функция f является сильной, если значения $DP^f_{\max}$ и $DL^f_{\max}$ функции f являются достаточно малыми [14].

Нас в дальнейшем и будут интересовать значения $DP^f_{\max}$ и $DL^f_{\max}$ для случаев, когда в качестве функции f выступают цикловые преобразования и последовательности цикловых преобразований итеративных шифров (ключезависимые функции), а также подстановочные преобразования (неключезависимые функции).

Пусть π – подстановочная таблица с n-битными входами и n-битными выходами. В [8] доказана лемма 1

Лемма 1. *Для любого преобразования* π: $Z_2^n \to Z_2^n$

$$\sum_{\Delta y \in Y} DP^{\pi}(\Delta x \to \Delta y) = 1, \quad (5)$$

$$\sum_{x \in X} LP^{\pi}(\ x \to\ y) = 1. \quad (6)$$

И, более того, *если* π *– подстановка, то*

$$\sum_{\Delta x \in X} DP^{\pi}(\Delta x \to \Delta y) = 1, \quad (7)$$

$$\sum_{y \in Y} LP^{\pi}(\ x \to\ y) = 1. \quad (8)$$

Эти результаты представляются достаточно очевидными, исходя из определений (1) и (2), примененных к подстановкам (неключезависимым преобразованиям). Они являются отражением известных фактов, заключающихся в том, что суммы ячеек таблицы XOR разностей и суммы квадратов ячеек таблиц линейных аппроксимаций подстановок по строкам и по столбцам равны 2^n и $\left(2^{n-1}\right)^2$ соответственно, где n – битовый размер входа и выхода подстановки порядка 2^n. Важным для дальнейшего является понятие случайной подстановки. Мы на нем остановимся отдельно.

2. СЛУЧАЙНЫЕ ПОДСТАНОВКИ

Напомним, что ранее в нашей работе [15] понятие случайной подстановки было определено следующим образом.

Определение 1. *Под случайной* (*квазислучайной*) *подстановкой понимается подстановка, которая удовлетворяет одновременно трем критериям случайности:*

1. *Число инверсий* η_n *в подстановке степени* n *приблизительно равно числу "антиинверсий", а практически, если*

$$\left|\eta_n - \frac{n(n-1)}{4}\right| \le a\sigma_\eta,\ \sigma_\eta = \frac{n^{3/2}}{6}.$$

2. *Число циклов* ξ_n *в подстановке степени* n *близко к* $\ln n$, *а практически, находится в границах*

$$\left|\xi_n - \ln n\right| \le a\sigma_\xi,\quad \sigma_\xi = \sqrt{\ln n}\ .$$

3. *Число возрастаний* θ_n *в подстановке степени* n *приблизительно равно числу убываний, а практически*

$$\left|\theta_n - \frac{n}{2}\right| \le a\sigma_\theta,\ \sigma_\theta = \sqrt{n/12}.$$

В этих соотношениях a – параметр, выбираемый в значительной степени из субъективных соображений (по крайней мере, из условия, что множество допустимых подстановок не станет меньше некоторого практически целесообразного числа). В наших предложениях использовалось значение $a = 1$. Остается заметить, что из полного множества подстановок порядка 2^n в этом случае приведенные критерии отбора проходят 53% всех подстановок.

В последующих наших публикациях [16, 18], посвященных исследованию дифференциальных и линейных свойств случайных подстановок и подстановочных преобразований, развивающих результаты работ Luka O'Connor-a [17, 19], мы определили еще два условия, которым подчиняются случайные подстановки. Они основываются на двух утверждениях. Напомним здесь их, так как они являются важными для дальнейшего.

В обозначениях работы [16] пусть $\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)$ будет вероятностью того, что значение ячейки дифференциальной таблицы случайно взятой подстановки π порядка 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно $2k$. Эта вероятность определяется теоремой.

Утверждение 1. *Для любых ненулевых фиксированных* ΔX, $\Delta Y \in Z_2^n$ *в предположении, что подстановка* π *выбрана равновероятно из множества* S_2^n *и* $0 \le k \le 2^{n-1}$,

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = \left(\begin{matrix} 2^{n-1} \\ k \end{matrix}\right)^2 \cdot \frac{k! \cdot 2^k \cdot \Phi(2^{n-1} - k)}{2^n!}, \quad (9)$$

где функция $\Phi(d)$ определяется выражением

$$\Phi(d) = \sum_{i=0}^{d} (-1)^i \cdot \left(\begin{matrix} d \\ i \end{matrix}\right)^2 \cdot 2^i \cdot i! \cdot (2d - 2i)!. \quad (10)$$

Закон распределения вероятностей (9) получен для полного множества подстановок, однако замечательным его свойством является то, что он оказывается справедливым и для усеченного (причем, существенно) множества подстановок, формируемых симметричными шифрами. Такие преобразования, осуществляемые на различных ключах зашифрования, формируют множество подстановок случайного типа (это основное свойство, к которому стремятся разработчики

при построении шифра). Об этом свидетельствуют и многочисленные результаты экспериментов. И это еще не все! Получается, что для множества подстановок, определяемых шифрующими преобразованиями, выполняется свойство, напоминающее эргодическое свойство случайных процессов (среднее по множеству реализаций совпадает со средним по времени для одной достаточно длинной реализации [20]). Это свойство проявляется в том, что закон распределения (9), полученный на основе анализа всего множества $2^n!$ равновероятных подстановок, является справедливым и для множества ячеек таблицы XOR разностей каждой отдельно взятой случайной подстановки степени 2^n.

Подтверждением этого факта является то, что для закона вероятностей $\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)$, рассматриваемого применительно к отдельной подстановке, с высокой точностью выполняется условие нормировки, характерное для полной группы событий

$$\sum_{k=0}^{k^*}\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)=1. \qquad (11)$$

Здесь $\Lambda_\pi(\Delta X,\Delta Y)$ – значение XOR таблицы (её ячейки) для пары значений разностей входов и выходов $\Delta X,\Delta Y\in Z_2^m$, $\Delta X=X+X'$, $\Delta Y=\pi(X)+\pi(X')$ подстановки $\pi\in S_2^m$. Значение k^* представляет собой половину от максимального числа переходов XOR таблицы случайной подстановки (фактически соотношение (11) – это обобщение свойств (5)-(8)). Выполненные многочисленные проверки подтверждает и это положение.

Совершенно аналогичное по содержанию утверждение, справедливо для вероятности значений линейных аппроксимационных таблиц $LAT_\pi^*(\alpha,\beta)$ случайных подстановок [19, 21].

Утверждение 2. *Пусть* $\lambda^*(\alpha,\beta)$ *будет случайным значением распределения* $LAT_\pi^*(\alpha,\beta)=\left|LAT_\pi(\alpha,\beta)-2^{n-1}\right|$, *когда подстановка* π *выбрана равновероятно из множества* 2^n *и маски* α,β *не нулевые. Тогда* $\lambda^*(\alpha,\beta)$ *принимает только четные значения и*

$$\Pr(\lambda^*(\alpha,\beta)=2k)=\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\begin{pmatrix}2^{n-1}\\ 2^{n-2}+|k|\end{pmatrix} \qquad (12)$$

для $|k|\le 2^{n-2}$.

И для этого распределения справедлива нормировка

$$\sum_{k=0}^{k^*}\Pr(\lambda^*(\alpha,\beta)=2k^*)=1. \qquad (13)$$

Здесь k^* – половинное значение максимального для таблицы $LAT_\pi^*(\alpha,\beta)$ смещения.

Более того, можно убедиться, что для распределения (12) справедлива и нормировка (8), которая в этом случае записывается в виде

$$\frac{2^n-1}{\left(2^{n-1}\right)^2}\cdot\sum_{k=-2^{n-1}}^{2^{n-1}}\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\begin{pmatrix}2^{n-1}\\ 2^{n-2}+|k|\end{pmatrix}^2=1. \qquad (14)$$

На основе изложенных результатов представляется логичным в дополнение к уже известным подходам сформировать (сформулировать) новое (или уточненное) определение случайной подстановки, что и сделано в работе [23]. Мы здесь его напомним.

Определение 2. *Подстановка является случайной, если вместе с выполнением трех критериев случайности, предложенных в работе* [24], *для ячеек её XOR таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей* (9) (*критерий случайности* 4) *и* (12) (*критерий случайности* 5).

3. ШИФРУЮЩИЕ ПРЕОБРАЗОВАНИЯ КАК СЛУЧАЙНЫЕ ПОДСТАНОВКИ

Самый важный вывод работ [15] и [17] состоит в том, что приведенные выше критерии случайности подстановок выполняются и для шифрующих преобразований всех современных блочных симметричных шифров, рассматриваемых как подстановочные преобразования.

Само по себе отдельное шифрующее преобразование (отдельный цикл) не является случайной подстановкой, так как для него не выполняются законы распределения вероятностей (9) и (12). Оно не укладывается в рамки случайных подстановок и по инверсиям, и по возрастаниям, и по циклам (хотя бы потому, что имеются множества входов в подстановку, которые влияют не на все значения выходов). Однако при реализации механизмов перемешивания (линейных преобразований), используемых в каждом цикле, последовательность шифрующих преобразований приобретает свойства случайной подстановки (к чему как раз и стремятся все разработчики шифров). Этот, казалось бы, тривиальный вывод остался не замеченным разработчиками шифров и криптоаналитиками при формировании оценок показателей стойкости шифров к атакам дифференциального и линейного криптоанализа (они не могли правильно интерпретировать результаты, так как были связаны полномасштабными версиями шифров, не поддающимися вычислительным экспериментам). Как уже отмечалось выше, во всех известных работах показатели многоцикловых преобразований (стойкость к атакам дифференциального и линейного криптоанализа) непосредственно связывались и связываются с соответствующими показателями S-блоковых конструкций, используемых в качестве нелинейных преобразований каждой цикловой функции.

Наша позиция состоит в том, что итоговые (асимптотические) показатели стойкости (максимумы полных дифференциалов таблиц XOR разностей последовательностей шифрующих преобразований также как и максимумы линейных аппроксимационных таблиц этих же преобразова-

ний) зависят только от числа циклов шифрующего преобразования и размера его битового входа.

Зафиксируем этот вывод в виде утверждения.

Утверждение 3. *Для каждого блочного симметричного шифра* (*из числа известных итеративных БСШ*) *существует вполне определенное число циклов, после которого шифр приобретает свойства случайной подстановки. Дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные и линейные свойства шифра. Это значение является одним и тем же для всех шифрующих преобразований с одинаковым битовым размером входа.*

Можно отметить, что это утверждение в первой части представляется в известном смысле достаточно очевидным в том смысле, что каждый реальный шифр строится так, чтобы набор его цикловых преобразований в той или иной мере обладал свойствами случайной подстановки. При нашем подходе это свойство определяется как промежуточный результат, переходящий в асимптотическое значение одинаковое для всех шифров (с одинаковым битовым размером входа), поддающийся расчету.

Нас в дальнейшем будет интересовать именно момент (число циклов), начиная с которого шифрующее преобразование становится случайной подстановкой. Именно в этом направлении мы и будем строить доказательство (обоснование) представленного утверждения.

Продемонстрируем справедливость этого утверждения на примере рассмотрения дифференциальных показателей шифра-подстановки. В качестве одного из таких показателей в нашем случае будет выступать максимальное значение полного дифференциала.

Мы начнем доказательство этого утверждения (скорее не доказательство, а объяснение его правомерности) с конца, т.е. предположим, что БСШ имеет некоторое определенное число циклов, после которых шифр становится случайной подстановкой, т.е. обладает законом распределения вероятностей переходов разностей (9).

Покажем, что дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные свойства этого шифра.

Важно сразу отметить, что особенностью случайной подстановки, удовлетворяющей критерию 4, является то, что мы имеем дело не с фиксированным распределением переходов разностей $\Delta x \to \Delta y$ (закрепленным распределением значений входов (ячеек) таблицы XOR разностей), а со случайным. Таблица XOR разностей случайной подстановки определяется тем, что для нее является фиксированным число ячеек каждого типа, определяемых с помощью закона распределения $\Pr\left(\Lambda_f(\Delta x,\Delta y)=2k\right)$ в виде [15]

$$\Lambda_{m,2k} = (2^m-1)^2 \cdot \Pr(\Lambda_f(\Delta x,\Delta y) = \\ = \frac{(2^m-1)^2}{2^m!}\cdot\begin{pmatrix}2^{m-1}\\ k\end{pmatrix}^2 \cdot k!\cdot 2^k \cdot \Phi(2^{m-1}-k). \qquad (15)$$

В соответствии с этим соотношением таблица XOR разностей случайной подстановки имеет λ_0 ячеек, имеющих значение $\Lambda_{m,0}$, λ_1 ячеек, имеющих значение $\Lambda_{m,2}$, λ_2 ячеек, имеющих значение $\Lambda_{m,4}$, и т.д., – $\lambda_{k_f^*}$ ячеек, имеющих значение $\Lambda_{m,2k^*}$. Все эти значения вместе дают общее число ненулевых входов (ячеек) в подматрицу таблицы XOR разностей равное $2^{n-1}\times 2^{n-1}$, причем сами числа $\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_{k_f^*}$ определяются однозначно из (15).

Поэтому применительно к шифрующим многоцикловым преобразованиям – случайным подстановкам, – дифференциальные вероятности DP^f должны теперь интерпретироваться в обозначениях подстановочных преобразований для ключезависимой функции f не как фиксированные, а как случайные значения, принимаемые на множестве ключей зашифрования (на множестве подстановок)

$$DP^f(\Delta x,\Delta y) = DP^f(\Delta x \to \Delta y) = \\ = \Pr\left(\Lambda_f(\Delta x,\Delta y)=2k\right) \to \qquad (16) \\ \to\ DP^f\left(\Lambda_f(\Delta x,\Delta y)=2k\right),$$

причем эти вероятности следует считать одинаковыми для всех ячеек таблицы дифференциальных разностей (для всех вариантов фиксированных сочетаний входных и выходных разностей).

Возвратимся к нашей задаче. Итак, пусть r-цикловое шифрующее преобразование (последовательность r-цикловых преобразований) f_r с n-битным размером входа (и выхода) обладает свойством 4, т.е. закон распределения $DP^{f_r}(\Delta x,\Delta y)$ переходов входных разностей Δx в выходные разности Δy имеет вид (9) с нормировкой

$$\sum_{k=0}^{k^*} DP^{f_r}\left(\Lambda_f(\Delta x,\Delta y)=2k\right)=1.$$

Тогда, если на входы очередного циклового преобразования (подстановки) поступают некоторые сочетания пар выходов предшествующего преобразования случайного типа (предшествующей случайной подстановки) подчиняющиеся закону распределения XOR разностей таблицы полных дифференциалов (9), то цикловое преобразование может осуществить лишь переименование выходов и соответствующих им разностей, оставляя результирующий закон распределения разностей неизменным (для операции XOR подстановка вместе с последующим или предыдущим линейным цикловым преобразованием являются детерминированными преобразованиями и произведение случайной в оговоренном смысле подстановки на любую другую подстановку, является случайной подстановкой). Приведем математическое обоснование этого факта (который подтверждается многочисленными экспериментами с малыми шифрами).

Нас интересует закон распределения вероятностей $DP^{f_{r+1}}(\Delta x,\Delta z)$ для $r+1$ цикла преобразований (здесь удобнее будет перейти к компактной

форме записи, введенной ранее), где Δz является выходной разностью $r+1$-но циклового преобразования. У нас имеется цепочка $\Delta x \to \Delta y \to \Delta z$ разностей, совместный закон распределения вероятностей для которой обозначим:

$$DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z) = DP^{f_{r+1}}(\Delta x \to \Delta y \to \Delta z).$$

В соответствии с формулой умножения вероятностей можем записать представление для этой вероятности в виде:

$$DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z) =$$
$$= DP^{f_r}(\Delta x, \Delta y) DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

Тогда дифференциальная вероятность $DP^{f_{r+1}}(\Delta x, \Delta z)$ для $r+1$-но циклового преобразования может быть определена из совместной вероятности $DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z)$ путем ее усреднения по множеству промежуточных значений $\Delta y \in Z_2^n$, т.е.

$$DP^{f_{r+1}}(\Delta x, \Delta z) =$$
$$= \sum_{\Delta y \in Z_{2^n}} DP^{f_r}(\Delta x, \Delta y) DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

Но в нашем случае закон распределения $DP^{f_r}(\Delta x, \Delta y) = \Pr\left(\Lambda_f(\Delta x, \Delta y) = 2k\right)$ является одним и тем же для каждой выходной разности r-циклового преобразования (для каждой ячейки таблицы дифференциальных разностей случайной подстановки), а поэтому

$$DP^{f_{r+1}}(\Delta x, \Delta z) =$$
$$= DP^{f_r}(\Delta x, \Delta y) \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

Очевидно далее, что при фиксированных значениях Δy выходные разности Δz не зависят от того, какие значения принимают входные разности Δx и, следовательно,

$$\sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta x, \Delta y) = \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta y) =$$
$$= \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta y \to \Delta z).$$

Но в соответствии с (5) для подстановочного одноциклового преобразования f_1

$$\sum_{\Delta y \in Y} DP^{f_1}(\Delta x, \Delta y) = \sum_{\Delta y \in Y} DP^{f_r}(\Delta x \to \Delta y) = 1,$$

и, в итоге, приходим к результату

$$DP^{f_{r+1}}(\Delta x, \Delta z) = DP^{f_r}(\Delta x, \Delta y) \Rightarrow$$
$$\Rightarrow DP^{f_{r+1}}(\Delta x \to \Delta z) = DP^{f_r}(\Delta x \to \Delta y),$$

где

$$DP^{f_r}(\Delta x \to \Delta y) = \Pr\left(\Lambda_f(\Delta x, \Delta y) = 2k\right).$$

Последнее и обозначает, что дополнительные цикловые преобразования уже не изменяют закона распределения разностей на выходе шифра.

Остается теперь прокомментировать первую часть утверждения. Для этого заметим, что эффективность перемешивания входного текста при зашифровании в криптографии оценивается такими параметрами статистической безопасности, как лавинный эффект, коэффициент сжатия, ряд корреляционных показателей [21].

Если рассматривать тонкую структуру циклового преобразования, то в самом начале процедуры зашифрования (в первом цикле) при применяемых при построении большинства шифров решений, как правило, не удается реализовать связь каждого выходного бита циклового преобразования с каждым входным битом. Например, биты входа влияют на вход только одного S-блока многоблочного нелинейного преобразования, а используемое последующее линейное преобразование не обладает полнотой в том смысле, что оно передает воздействие входа не на все выходы текущего преобразования. Для характеристики этого свойства разработчики шифра Rijndael ввели специальную характеристику – коэффициент ветвления, а сам механизм распространения активных битов в последовательных слоях (циклах) преобразований назвали стратегией широкого следа [22]. Но эту же стратегию пытались реализовать все разработчики известных шифров, хотя она была часто не такой эффективной, как, скажем, у Rijndael-я (умножение выходов нескольких S-блоков на матрицу МДР кода). С другой стороны, известны и более эффективные конструкции линейного слоя (например, в шифре Лабиринт, или в шифре управляемой подстановки [25]). Естественно, что если есть механизм расширения числа активных (задействованных) в ходе преобразования битов блока данных, то рано или поздно наступит момент, когда любой бит входа будет одинаково эффективно действовать на любой бит выхода. Этот момент как раз и будет обозначать, что шифрующее преобразование стало случайной подстановкой (результирующий закон распределения переходов разностей пар входов в соответствующие им разности пар выходов принимает вид (9)).

Совершенно аналогичные рассуждения могут быть приведены по отношению к линейным показателям многоцикловых итеративных процедур шифрующих преобразований.

4. РАСЧЕТНЫЕ СООТНОШЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЕЙ СТОЙКОСТИ К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Расчетные соотношения для определения максимальных значений полных дифференциалов и максимальных значений линейных корпусов могут быть получены применением законов (9) и (14), справедливых для случайных подстановок, к шифрам, рассматриваемым как случайные подстановки, что и сделано в наших работах [16] и [18].

Как показано в работе [16], среднее значение максимума таблицы XOR разностей случайной подстановки порядка 2^n находится путем определения максимального значения $k = k_{\max}$, при котором выполняется соотношение

$$\frac{(2^n-1)^2}{2^n!}\cdot\binom{2^{n-1}}{k}^2\cdot k!\cdot 2^k\cdot\Phi(2^{n-1}-k)\approx 1. \quad (19)$$

Если это соотношение применить к шифру с n-битовым размером входа, то для интересующего нас максимального значения дифференциальной вероятности (максимальной вероятности полного дифференциала) $DP^f_{\max}$ можем записать выражение

$$DP^f_{\max}=\frac{k_{\max}}{2^n}. \quad (20)$$

В работе [16] также приведено расчетное соотношение, являющееся хорошей аппроксимацией соотношений (19) и (21)

$$DP^f_{\max}=\frac{n+4}{2^n}. \quad (21)$$

В работе [18] показано, что среднее значение максимума таблицы линейных аппроксимаций для случайной подстановки определяется аналогично предыдущему случаю путем нахождения значения k^*, являющегося целым решением (округлением в сторону ближайшего целого) уравнения

$$\frac{(2^n-1)^2\cdot\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+|k^*|}=1. \quad (22)$$

Соответственно для шифра с n-битовым размером входа максимальное значение линейной вероятности (максимальной вероятности линейного корпуса) $DL^f_{\max}$ представляется в виде

$$DP^f_{\max}=\left(\frac{k_{\max}}{2^{n-1}}\right)^2. \quad (23)$$

Приведем здесь также соотношение, полученное на основе обработки результатов вычислительных экспериментов, являющееся удобной заменой выполнению расчетов по соотношению (22)

$$DL^f_{\max}=\left(\frac{\left(\frac{3}{2}\right)^n}{2^{n-1}}\right)^2. \quad (24)$$

ЗАКЛЮЧЕНИЕ

На основе приведенных результатов и обоснований можно утверждать, что:

1. Современные блочные симметричные шифры (при полном наборе шифрующих многоцикловых преобразований) обладают свойствами случайных подстановок и для них справедливы законы распределения вероятностей для полных дифференциалов и линейных корпусов свойственные таблицам дифференциальных разностей и линейных аппроксимаций подстановок соответствующей степени (порядка) (9) и (12).

2. Максимальные значения полных дифференциалов и линейных корпусов для современных БСШ, определяющие по современным меркам показатели стойкости шифров к атакам дифференциального и линейного криптоанализа, могут быть получены расчетным путем. Они не зависят (при достаточном числе цикловых преобразований ни от свойств используемых в шифрах подстановочных конструкций, ни от методов введения в цикловые функции цикловых подключей, ни от способа построения расширяющего линейного преобразования цикловой функции, а являются функцией только размера битового входа в шифр (порядка подстановки).

3. Для оценки стойкости блочных симметричных шифров (с битовым размером входа равным n) к атакам дифференциального и линейного криптоанализа можно пользоваться простыми соотношениями (23) и (24).

Литература.

[1] Thomas Baignoires and Serge Vaudenay Proving the Security of AES Substitution-Permutation Network. http://lasecwww.epfl.ch. 2004. p. 16.

[2] Liam Keliher. Toward Provable Security Against Differential and Linear Cryptanalysis for Camellia and Related Ciphers, International Journal of Network Security, Vol.5, No.2, pp.167–175, Sept. 2007.

[3] *L. Keliher, H. Meier, and S. Tavares.* New method for upper bounding the maximum average linear hull prodadility for SPNs, Advances in Cryptology – EUROCRYPT 2001, LNCS 2045, Springer-Verlag, pp. 420-436, 2001.

[4] *L. Keliher, H. Meijer, and S. Tavares,* Improving the upper bound on the maximum average linear hull probability for Rijndael, Eighth Annual International Workshop on Selected Areas in Cryptography (SAC 2001), LNCS 2259, pp. 112-128, Springer-Verlag, 2001.

[5] *Алексийчук А.Н., Ковальчук Л.В., Скрыпник Е.В., Шевцов А.С.* Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах // Прикладная радиоэлектроника. – 2008. – Т.7. – №3. – С. 203-209.

[6] Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004— Version 0.15 (beta), Springer-Verlag.

[7] *K. Nyberg and L. Knudsen,* Provable security against differential cryptanalysis, Journal of Cruptology, vol.8, no.1,1995.

[8] *M. Matsui.* On a Structure of Block Ciphers with Provable Security against Differential and Lintar Cryptanalysis. IEICE TRANS. FUNDAMENTALS, Vol. E82–A, NO. 1 JANUARY 1999, p. 117-122.

[9] *H. Feistel,* Cryptography and computer privacy. Scientific American, 228(5): 15-23,1973.

[10] *Долгов В.И., Лисицкая И.В., Олейников Р.В.* Подход к криптоанализу современных шифров // Материалы второй международной конференции "Современные информационные системы. Проблемы и тенденции развития", Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435-436.

[11] *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. – 2007. Том. 6, №2, С. 230-240.

[12] *Горбенко І.Д., Бондаренко М.Ф., Долгов В.И., Олійников Р.В., Руженцев В.І., Міхайленко М.С., Колесников П.О.* Перспективний блоковий симетричний шифр

"Мухомор" – основні положення та специфікація // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 2. – С. 147-157.

[13] *Горбенко І. Д., Долгов В.І., Олійников Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Тоцкій О.С., Казьміна С.В.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація // Прикладная радиоэлектроника. – 2007. – Т.6. – № 2. – С. 195-208.

[14] *Кузнецов А.А., Сергиенко Р.В., Наумко А.А.* Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) // Прикладная радиоэлектроника. – 2007. – Т.6. – № 2. – С. 241-249.

[14] *F. Sano, K. Ohkuma, H. Chimisu, and S. Rawamura*. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis, IEISE Trans. Fundamentals, VOL. E86-A, No.1, pp. 37–46, Janiary 2003.

[15] *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 //. Радиотехника. Всеукр. межвед. науч.-техн. сб. 1997. Вып 103. С. 121–130.

[16] *Олейников Р.В., Олешко О.И., Лисицкий К.Е.* Дифференциальные свойства случайных подстановок // Прикладная радиоэлектроника: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 326-333.

[17] *L.J. O'Connor.* On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, vol. 795, T. Hellesethed., Springer-Verlag, pages 360–370, 1994.

[18] *Долгов В.И., Лисицкая И.В., Олешко О.И.* Свойства таблиц линейных аппроксимаций случайных подстановок // Прикладная радиоэлектроника: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 334-340.

[19] *Luke O'Connor.* Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995.

[20] *Вентцель Е.С.* Теория вероятностей. – М.: Наука, 1964. – 564 с.

[21] *Luke O'Connor.* On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995. (семь страниц).

[22] *Бронштейн И.Н., Семендяев К.А.* Справочник по математике для инженеров и учащихся вузов. Издво – М:. "Наука" 1980. – 976 с.

[23] *Долгов В.И., Лисицкая И.В., Лисицкий К.Е.* Случайные подстановки в криптографии. Доклад, представленный на конференцию. Кировоград, 2010.

[24] *Лисицкая И.В.* К вопросу построения долговременных ключей для алгоритма ГОСТ 28147-89 // Информационно-управляющие системы на железнодорожном транспорте. 1997. № 3. С. 54–57.

[25] *Долгов В.И., Лисицкая И.В., Казимиров А.В.* Вариации на тему шифра Rijndael. // Прикладная радиоэлектроника: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 321-325.

Поступила в редколлегию 21.06.2010.

Горбенко Иван Дмитриевич, доктор технических наук, профессор, заведующий кафедрой БИТ ХНУРЭ, главный конструктор ЗАО «Институт информационных технологий». Область научных интересов: криптографические системы и протоколы, проектирование и разработка систем, комплексов и средств криптографической защиты информации.

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Олейников Роман Васильевич, кандидат технических наук, докторант кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

УДК 681.3.06

Нова ідеологія оцінки стійкості блокових симетричних шифрів до атак диференційного і лінійного криптоаналізу / І.Д. Горбенко, В.І. Долгов, І.В. Лисицька, Р.В. Олійников // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 312-320.

Пропонується підхід до оцінки безпеки блокових шифрів, що орієнтується, з одного боку, на використання при визначенні очікуваних показників стійкості блокових шифрів результатів аналізу показників їх зменшених версій, а з іншого, на використання уточненої в останній час на основі дослідження властивостей та показників випадкових підстановок і зменшених моделей шифрів, які розглядаються як підстановочні перетворення, концепції (нової ідеології) визначення показників стійкості блокових шифрів до атак диференційного та лінійного криптоаналізу .

Ключові слова: диференційний і лінійний криптоаналіз, показники стійкості до атак лінійного і диференційного криптоаналіза, властивості випадкових підстановок і перетворень, що шифрують.

Бібліогр.: 25 найм.

UDC 681.3.06

A new ideology of evaluating block symmetric ciphers strength to differential and linear cryptanalysis attacks / I.D. Gorbenko, V.I. Dolgov, I.V. Lisitskaya, R.V. Oleinikov // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 312-320.

An approach to evaluating the security of block ciphers is suggested which, on the one hand, is oriented on the use of the results of analyzing the reduced versions of big ciphers in determining the anticipated strength indices of the said big ciphers and, on the other hand, on the concept (new ideology) of determining the indices of block symmetric ciphers strength to attacks of differential and linear cryptanalysis, which has been lately defined more exactly on the basis of studying the properties and indices of random substitutions and reduced models of ciphers considered as substitution transformations.

Key words: differential and linear cryptanalysis, strength indexes to differential and linear cryptanalysis attacks, properties of random substitutions and encryption transformations.

Ref.: 25 items.

УДК 621.3.06

ВАРИАЦИИ НА ТЕМУ ШИФРА RIJNDAEL

В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, А.В. КАЗИМИРОВ

Рассматривается подход к анализу показателей криптографической стойкости блочных симметричных шифров, строящийся на основе исследования свойств уменьшенных версий этих шифров. С использованием этого подхода оцениваются показатели стойкости к атакам дифференциального криптоанализа нескольких модификаций SPN шифра с 16-битным входом, имеющего структуру общего типа, предложенную в работе Говарда Хейса. Показывается, что существуют решения, превосходящие по показателям стойкости шифр Rijndael.

Ключевые слова: симметричный блочный шифр, криптоанализ, Rijndael.

ВВЕДЕНИЕ

В нашей предыдущей работе [1] мы подняли вопрос о перспективности и новизне решений, использованных при построении шифра Rijndael. Было отмечено, что этот шифр практически повторяет не только общую структуру SPN шифра, рассмотренную в работе Х. Фейстеля 1973 года [2], но и практически по стойкости (при полном наборе цикловых преобразований) оказывается ничуть не лучше своего исторического прототипа. Он представляется выигрышным по сравнению с классической схемой (в 16-битной интерпретации работы [3]) только в динамике выхода на асимптотические показатели стойкости к атакам дифференциального (и линейного) криптоанализа (четыре цикла против семи). Этот выигрыш достигается за счет более эффективного линейного преобразования, примененного в цикловой функции, реализующего стратегию широкого следа (умножения на матрицу МДР кода и циклического сдвига векторов состояний).

В этой работе мы хотим привлечь внимание еще к одному аспекту оценки перспективности решений, заложенных в шифр Rijndael, а именно нас будет интересовать построение преобразования более эффективного, чем реализуется в стандарте 21-го века! Мы приведем примеры таких решений.

1. ОПИСАНИЕ ВАРИАНТОВ РЕАЛИЗАЦИЙ SPN ШИФРОВ

В основе всех последующих рассмотрений будет использована обобщенная структура 16-битного SPN шифра Фейстеля в интерпретации работы [2]. Она приведена на рис. 1. Модификации этой SPN структуры будут состоять в использовании различных вариантов начального и конечного (IT и FT) преобразований.

В частности будут рассмотрены начальные и конечные преобразования двух типов. Первое будет повторять уменьшенные версии начального и конечного преобразований шифра Лабиринт [4]. Мы здесь кратко напомним сущность этих преобразований, описанных в нашей работе [5].

Начальное IT преобразование уменьшенной версии шифра «Лабиринт» (рис. 2) включает сложение по модулю 2^{16} входного 16-битного блока данных с 16-битным подключом. На следующем шаге 16-ть результирующих бит разбиваются на блоки по 4-е бита, которые подаются на нелинейные преобразования, осуществляемые S-блоками. Далее 4-х битные выходы S-блоков объединяются в новые 16-ть бит и опять разбиваются на два полублока, над которыми выполняются циклические сдвиги:левый полублок сдвигается на 4 бита влево, а правый соответственно на четыре бита вправо, и в заключение над полученным 16-битным блоком выполняется операция инволютивного линейного смешивания IMix на 2 бита. Результат предыдущего действия XOR-ится с левыми и правыми 8-ю битами входного слова.

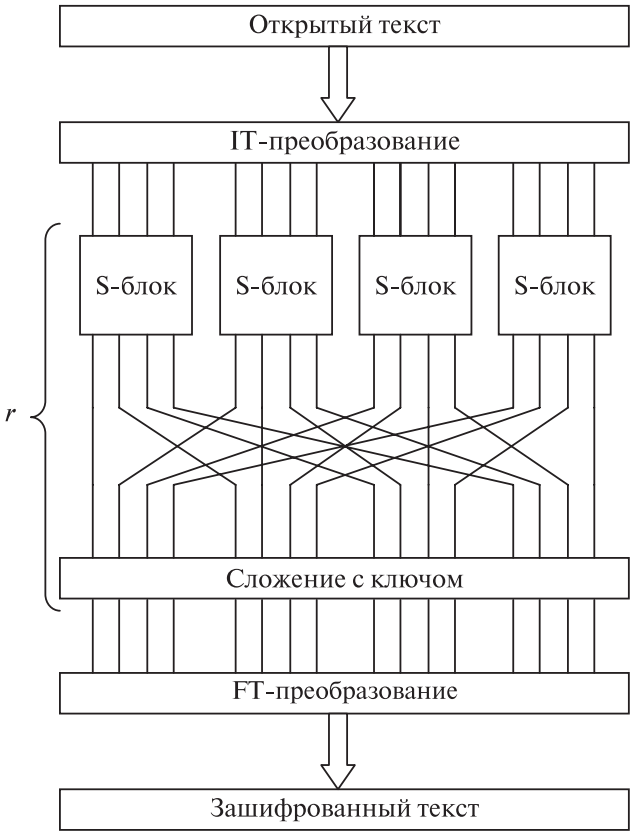


Рис. 1. Общий вид алгоритма Хейса.
На этом рисунке IT – начальное преобразование;
FT – конечное преобразование;
S-блок – подстановка полубайт в полубайт;
r – количество циклов

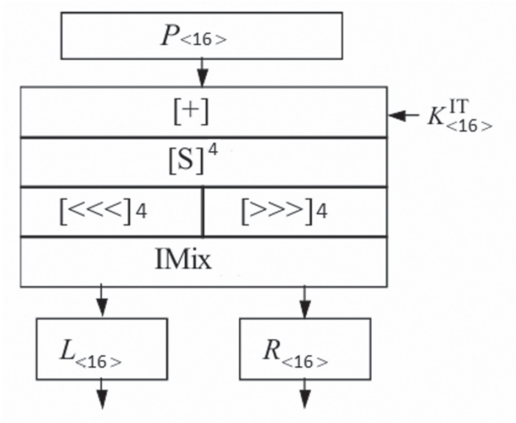


Рис. 2. Начальное преобразование IT

В уменьшенной версии шифра операция IMix реализуется следующим образом: складываются по модулю два левые 8 бит с правыми входных данных, после, результат сдвигается циклически влево.

Конечное FT преобразование (рис. 3) выполняет те же операции, что и начальное, но только в обратном порядке.

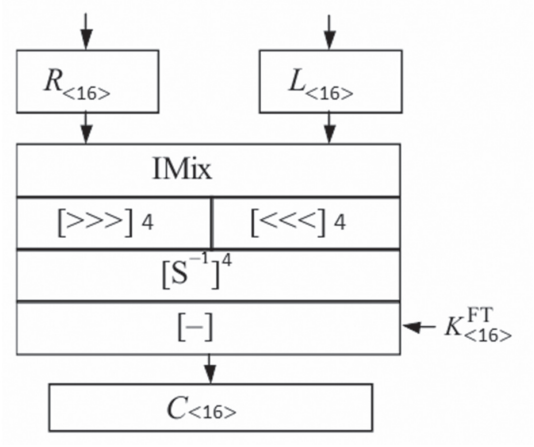


Рис. 3. Конечное преобразование FT

Второй тип начального и конечного преобразований строится на основе идеи, изложенной в нашем патенте «Недетермінований спосіб криптографічного перетворення блоків даних» [6].

Здесь имеется в виду предложение по построению циклового преобразования с управляемыми подстановками, причем управление осуществляется в отличие от известных подходов не с помощью битов циклового подключа, а на основе использования в качестве управляющего воздействия результата нелинейного преобразования предыдущего S-блока. В этом случае в качестве таблиц нелинейной замены (S-блоков) используются сразу целые наборы противоречивых подстановок, называемые в математической литературе латинскими прямоугольниками [7]. Идею предлагаемого способа построения преобразования с управляемыми подстановками (в 16-битной редакции) поясняет рис. 4.

Входной 16-битный блок данных разбивается на 4-х битные подблоки B_0, B_1, B_2, B_3 и осуществляется поочередное преобразование подблоков на основе наборов управляемых подстановок в виде латинских прямоугольников размером $2^4 \times 2^4$.

Одним (″информационным″) входом в латинский прямоугольник является текущий подблок данных B_i, а вторым (″управляющим″) входом является результат (4-х битный блок), полученный на предыдущем шаге преобразования. В качестве инициализирующего подблока выступает вектор инициализации IV_1 (4-х битная константа). Преобразование на основе управляемой подстановки выполняется в обе стороны (двумя слоями). Перед первым слоем осуществляется операция сложения по модулю 2 с подключом. Очевидно, что потребуется вектор инициализации и для второго слоя преобразований. В качестве такового может выступать константа IV_2, либо B_3 или выход последней подстановки предыдущего слоя. На рис. 5 представлена схема реализации второго слоя преобразований с управляемыми подстановками.

3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

Далее мы будем интересоваться показателями стойкости шифров к атакам дифференциального крипоанализа в виде максимального значения их полных дифференциалов. Оценим сначала влияние на значения полных дифференциалов оговоренных выше конструкций шифрующих преобразований вида (м.б. моделей) S-блоков (известных и случайно сгенерированных), использованных

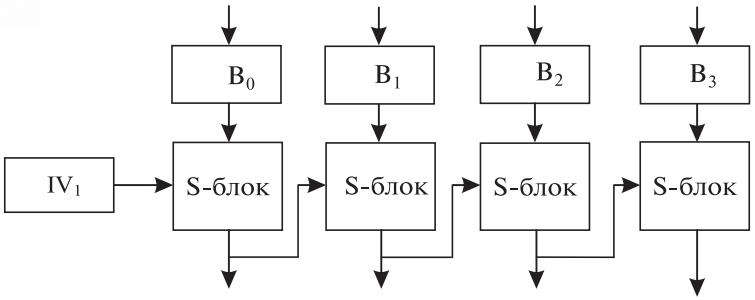


Рис. 4. Слой преобразования с управляемыми подстановками (16-битный вариант)

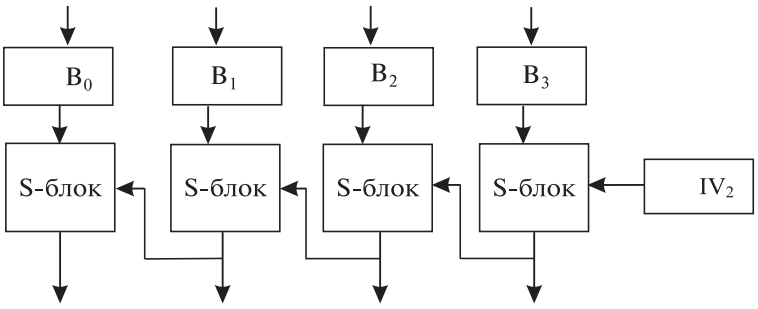


Рис. 5. Второй слой преобразований с управляемыми подстановками

при реализации каждой из конструкций. Список S-блоков, примененных в вычислительных экспериментах, приведен ниже в табл. 1.

Таблица 1

Варианты использованных S-блоков с расшифровкой их описаний

Варианты использованных S-блоков	Расшифровка описания S-блоков
SboxAESD4 ={A,4,3,B,8,E,2, C,5,7,6,F,0,1,9,D}; SboxHEYS D8 ={E,4,D,1,2,F, B,8,3,A,6,C,5,9,0,7}; SboxD6F2 = {B,C,5,0,1,3,2,7,8, 4,D,F,6,9,E,A}; SboxD6F0 = {4,6,F,B,E,7,5, D,9,C,1,0,3,8,A,2}; SboxD12F0 = {8,3,1,9,A,B,E, C,5,D,F,2,0,4,7,6}; SboxD8F0 = {C,9,4,6,8,E,D,5, 3,F,B,0,A,2,1,7}.	DX – X максимальное значение в дифференциальной таблице S-блока; FY – Y количество фиксированных точек ($S(x)=x$). Отсутствие FY в описании S-блока эквивалентно F0.

В их числе представлены S-блок мини версии шифра AES [8], S-блок шифра из работы [3] (первая строка S-блока шифра DES), остальные S-блоки сгенерированы случайным образом (выбраны из случайно сгенерированных S-блоков). Во всех вариантах рассматриваемых в дальнейшем конструкций шифров будут использоваться одни и те же (одинаковые) наборы S-блоки.

Первая серия экспериментов была проведена с 16-битным SPN шифром в том виде, в котором он представлен в работе проф. Хейса, где в качестве начального и конечного преобразований используется простое побитное сложение с цикловыми 16-битными подключами (начальное преобразование в виде $M = P \oplus K_0$ и конечное в виде $C = M' \oplus K_{r+1}$). Полученные значения полного дифференциала для различных вариантов S-блоков в зависимости от числа циклов преобразования представлены в табл. 2.

Анализ результатов показывает, что все варианты S-блоков, кроме последнего, выходят на асимптотическое значение максимума полного дифференциала в пределах первых девяти циклов итеративных преобразований. В то же время нашелся S-блок, который не достиг асимптотического значения на тринадцати циклах, однако это скорее исключение, чем правило (этот S-блок выходит за рамки случайного и по числу инверсий – 75 и не укладывается в границы случайного по критерию 4: он имеет 5 максимальных значений равных 8). Правда, не укладывается в рамки случайного и S-блок шифра мини AES (это одноцикловая подстановка с минимальным значением максимума XOR таблицы равным 4 и таких значений в таблице 15), а также не проходят критерий инверсий S-блоки SboxD6F0 и SboxD12F0.

Интересно отметить, что для S-блока SboxHEYSD8 асимптотическое значение 19 при нахождении полного дифференциала достигается на два цикла быстрее, чем для S-блока SboxAESD4 (S-блока, построенного по идеям разработчиков Rijndael).

Во второй серии экспериментов рассматривалась модель SPN шифра рис 1, в которой в качестве начального преобразования вместо операции XOR использовалось IT-преобразование вида $M = (P + K_0) \bmod 2^{16}$, при этом конечное преобразование FT не менялось, т.е. оно имело вид $C = M' \oplus K_{r+1}$. Соответствующие результаты расчётов представлены в табл. 3.

Сравнивая полученные результаты с таблицей 1, можно сделать вывод, что применение сложения по модулю 2^{16} в качестве начального преобразования существенных улучшений (более быстрого достижения асимптотического значения 19) не даёт).

Но в случае применения S-блоков SboxHEYSD8 заметно уменьшение значений полного дифференциала при числе циклов меньшем 7.

Далее было исследовано поведение значения полного дифференциала в случае, когда:

– начальное преобразование аналогично IT-преобразованию шифра «Лабиринт»;

– конечное преобразование имеет вид $C = M' \oplus K_{r+1}$.

Таблица 2

Значения полного дифференциала для различных S-блоков и количества циклов алгоритма Хейса

Sbox / r	SboxAESD4	SboxHEYSD8	SboxD6F2	SboxD6F0	SboxD12F0	SboxD8F0
1	16384,00	32768,00	24576,00	24576,00	49152,00	32768,00
2	4096,00	12288,00	6144,00	6144,00	15552,00	8192,00
3	2036,27	2303,33	2802,40	1920,00	1587,20	3432,00
4	596,00	222,27	649,33	601,20	613,13	1184,47
5	190,33	64,13	292,93	148,93	265,73	457,07
6	77,47	24,80	71,47	50,00	104,87	178,40
7	35,87	**18,80**	32,00	22,00	46,87	87,33
8	21,07	18,80	19,67	**19,07**	23,87	39,93
9	**19,27**	19,00	**18,93**	18,87	19,13	24,60
10	19,33	18,93	19,33	19,27	19,00	24,27
11	18,87	19,27	18,93	19,20	19,13	23,80
12	19,27	18,93	19,00	18,73	18,93	23,93
13	19,20	18,87	18,87	19,20	19,33	24,07

Таблица 3

Алгоритм Хейса с начальным сложением блоков данных с цикловым подключом (первичным забеливанием) по модулю 2^{16}

Sbox / №	SboxAESD4	SboxHEYSD8
1	16330,13	26016,60
2	3903,00	7403,60
3	1637,73	964,47
4	485,07	128,27
5	150,40	47,53
6	65,87	20,27
7	31,20	**19,07**
8	19,80	19,00
9	**19,07**	19,27
10	18,93	18,93
11	19,07	19,00
12	19,47	18,93
13	18,93	18,87

В этом эксперименте значение полного дифференциала при различном числе циклов преобразования имеет вид, представленный в табл. 4.

Таблица 4

Алгоритм Хейса с начальным IT-преобразованием шифра «Лабиринт»

Sbox / №	Sbox-D8F0	SboxHEYSD8	SboxAESD4
1	10068,87	7141,73	1234,13
2	1982,60	2229,20	313,07
3	549,73	296,33	127,67
4	220,80	37,93	47,67
5	94,00	**19,07**	22,80
6	42,33	19,33	**19,07**
7	22,47	19,20	19,40
8	**19,47**	19,20	19,40
9	19,27	19,07	19,00
10	19,53	18,87	19,00
11	19,47	19,27	19,00
12	19,67	19,00	19,33
13	19,47	19,27	19,47

Из таблицы видно, что использование IT-преобразования резко уменьшает количество циклов, необходимое для достижения значения 19. Даже при использовании S-блока SboxD8F0, который в первой серии экспериментов не достигал необходимого значения, теперь оно приходит к значению 19 при 8 циклах.

В табл. 5 представлены значения полного дифференциала, для случая, когда начальное и конечное преобразования эквивалентны преобразованиям IT и FT в шифре «Лабиринт».

Результаты таблицы 5 свидетельствуют, что применение IT и FT преобразований значительно уменьшает количество циклов, необходимых для достижения значения 19 по сравнению с оригинальными начальными и конечными преобразованиями, использованными в SPN шифре Хейса.

Таблица 5

Алгоритм Хейса с начальным IT-преобразованием и FT-преобразованием шифра «Лабиринт»

Sbox / №	Sbox-D8F0	SboxHEYSD8	SboxAESD4
1	733,13	517,13	517,20
2	132,93	76,87	40,67
3	25,67	23,93	20,20
4	20,07	**19,27**	**19,33**
5	**19,20**	19,27	18,93
6	18,67	19,27	19,53
7	19,27	18,93	19,07
8	19,07	18,93	19,07
9	19,00	19,13	19,13
10	19,53	19,33	19,20
11	19,00	19,07	18,93
12	19,13	19,00	18,87
13	19,40	19,00	18,93

Наконец, была проведена серия экспериментов, в которых было исследовано влияние на значения полного дифференциала применения в качестве IT и FT преобразований в структуре SPN шифра рис.1 управляемых подстановок в виде латинских прямоугольников. Результаты этих экспериментов иллюстрирует табл. 6.

Таблица 6

Алгоритм Хейса с преобразованиями, использующими латинский прямоугольник

Sbox / №	Sbox-D8F0	SboxHEYSD8	SboxAESD4
1	156,67	88	100,80
2	34,53	**18,87**	35,87
3	21,20	18,93	19,80
4	**19,13**	18,87	**19,07**
5	19,20	19,27	19,60
6	18,73	19,13	18,93
7	19,00	19,13	18,93
8	19,07	19,33	19,07
9	19,13	19,07	19,27
10	19,53	19,00	18,80
11	19,00	19,00	19,13
12	19,13	19,20	19,13
13	18,93	19,07	19,20

Из таблицы видно, что при применении слоев управляемых подстановок в качестве начального и конечного преобразований асимптотическое значение 19 достигается при минимальном числе циклов равном 2, что существенно эффективнее, чем в уменьшенной версии шифра мини-AES. Мы сделали для этого лучшего варианта просмотр максимальных значений полных дифференциалов для всех вариантов ключей. Результаты представлены в табл. 7.

При этом среднее значение полного дифференциала для 2-х циклового преобразования равно 19,11. Можно сделать вывод, что на двух циклах шифр приходит к асимптотическому значению.

Таблица 7

Максимальные значения дифференциалов двухцикловых характеристик

Мах значение полной диф. хар-ки	Их количество
18	31367
20	31962
22	2109
24	93
26	5

ЗАКЛЮЧЕНИЕ

Таким образом, на примере построения полных дифференциалов уменьшенных моделей 16-битного SPN шифра Хайса с различными начальными и конечными преобразованиями продемонстрирована возможность построения шифрующего преобразования более эффективного, чем реализованное в стандарте AES.

Однако, для того чтобы представлять общую картину, необходимо еще провести ряд дополнительных исследований: посмотреть, как будет себя вести с различными подстановками уменьшенная версия шифра Rijndael со случайными S-блоками и специально сгенерированными (удовлетворяющие критериям случайности), параллельно посмотреть ряд других алгоритмов (например, финалистов проекта NESSIE).

Литература.

[1] *Долгов В.И., Лисицкая И.В., Киянчук Р.И.* Rijndael – это новое или хорошо забытое старое? Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. II, С. 32-35.

[2] *Feistel, H.* Cryptography and Computer Privacy [Текст] / H. Feistel. // Scientific American. – May 1973. Vol. 228. – PP. 15–23.

[3] *H. M. Heys.* A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002, p 189-221.

[4] *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. Том. 6, № 2. – С. 230-240.

[5] *Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В.* Исследование циклических и дифференциальных свойств уменьшенной модели шифра «Лабиринт». // Прикладная радиоэлектроника: научн.-техн. журнал. – 2009. Том. 8, № 3. – С. 283-289.

[6] *Долгов В.І., Супронюк С.В., Лисицька І.В.* Спосіб недетермінованого криптографічного перетворення блоків даних. Деклараційний патент на винахід 53949 А, Бюл. № 2, від 17.02.2003.

[7] *Скачков В.Н.* Введение в комбинаторные методы дискретной математики. – М.: Наука – 1982 – 384 с.

[8] *Долгов В.И., Кузнецов А.А., Лисицкая И.В., Сергиенко Р.В., Олешко О.И.* Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров // Прикладная радиоэлектроника: научн.-техн. журнал. – 2009. – Т. 8. – №3. – С. 268-277.

[9] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Олешко О.И.* Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES // Прикладная радиоэлектроника: научн.-техн. журнал. – 2009. – Т. 8 № 3. – С. 252-257.

Поступила в редколлегию 23.06.2010.

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Казимиров Александр Владимирович, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

УДК 681.3.06

Варіації на тему шифра Rijndael / В.І. Долгов, І.В. Лисицька, А.В. Казимиров // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 321-325.

Розглядається підхід до аналізу показників криптографічної стійкості блокових симетричних шифрів, які будуються на основі дослідження властивостей зменшених версій цих шифрів. З використанням цього підходу оцінюються показники стійкості до атак диференційного криптоаналізу декількох модифікацій SPN шифра з 16-бітовим входом, який має структуру загального типу, що була запропонована у роботі Говарда Хейса. Показується, що існують рішення, що перевершують по показникам стійкості шифр Rijndael.

Ключові слова: симетричний блоковий шифр, криптоаналіз, Rijndael.

Табл. 07. Іл. 05. Бібліогр.: 09 найм.

UDC 681.3.06

Variations on Rijndael cipher theme / V.I. Dolgov, I.V. Lisitskaya, O.V. Kazimirov // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 321-325.

The paper considers an approach to the analysis of symmetric block ciphers cryptographic strength indices which is based on the research of the properties of reduced versions of these ciphers. Using this approach estimates strength indices to differential cryptanalysis attacks of several modifications of the 16-bit input SPN cipher haping a general type structure proposed in the work by Howard Heys. It is shown that there exist solutions which exceed the Rijndael in strength indices.

Key words: symmetric block cipher, cryptanalysis, Rijndael.

Tab. 07. Fig. 05. Ref.: 09 items.

УДК 621. 391:519.2:519.7

ДИФФЕРЕНЦИАЛЬНЫЕ СВОЙСТВА ПОДСТАНОВОК

Р.В. ОЛЕЙНИКОВ, О.И. ОЛЕШКО, К.Е. ЛИСИЦКИЙ, А.Д. ТЕВЯШЕВ

Выводятся расчетные соотношения для определения среднего значения максимумов XOR таблиц случайных подстановок. Показывается, что дифференциальные свойства современных блочных симметричных шифров (при заявленном числе циклов преобразования) являются одним из проявлений свойств случайных подстановок. Предлагается подход к сравнению эффективности решений по построению алгоритмов шифрования в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума полных дифференциалов.

Ключевые слова: симметричный блочный шифр, дифференциальный криптоанализ, случайная перестановка.

ВВЕДЕНИЕ

В наших предыдущих работах [1, 2] мы представляли результаты вычислительных экспериментов по исследованию дифференциальных свойств случайных таблиц подстановок. В частности, было установлено, что среднее значение максимумов таблиц XOR разностей является специфическим показателем S-блоков фиксированного порядка, не зависящим от циклового класса, к которому принадлежат подстановки.

Дальнейшие исследования [3, 4] показали, что это свойство является характерным и для шифрующих преобразований, выполняемых современными блочными симметричными шифрами, в то время как многие из подходов к оценке дифференциальных свойств шифров строятся на основе изучения свойств входящих в шифр подстановочных преобразований (S-блоков), а не шифров в целом как подстановок.

Учитывая жесткую связь дифференциальных свойств шифрующих преобразований с показателями их стойкости к атакам дифференциального криптоанализа, возникает желание более глубокого изучения накопленных фактов и осмысления имеющихся результатов.

В этой работе ставится задача теоретического обоснования полученных экспериментально дифференциальных показателей случайных подстановок, в качестве которых рассматриваются и блочные симметричные шифры.

Напомним, что в процессе экспериментов мы интересовались средним значением максимумов таблиц XOR разностей подстановок. Соответствующий показатель теперь необходимо определить расчетным путем.

1. ВЫВОД РАСЧЕТНЫХ СООТНОШЕНИЙ

Отметим сразу, что решение близкой по постановке задачи нам удалось найти в работе Luka O'Connor-a [5] 1994-го года. Однако манера представления материала Luka O'Connor-ом, особенно в части выполнения доказательств и интерпретации конечных результатов, нас не удовлетворила и сделала целесообразной изложение собственной позиции по этому вопросу.

Следуя работе [5], положим, что $\pi: Z_2^m \to Z_2^m$ является биективным m-битным отображением и пусть S_{2^m} будет множеством всех таких отображений, известное в математической литературе как симметрическая группа. Пусть $\Lambda_\pi(\Delta X, \Delta Y)$ будет значением XOR таблицы (её ячейки) для пары значений разностей входов и выходов ΔX, $\Delta Y \in Z_2^m$, $\Delta X = X + X'$, $\Delta Y = \pi(X) + \pi(X')$ подстановки $\pi \in S_{2^m}$.

Напомним, что XOR таблица представляет собой $2^m \times 2^m$ матрицу, у которой $XOR_\pi(i,j) = \Lambda_\pi(i,j)$, $0 \le i, j \le 2^{m-1}$.

Для m-битной подстановки π XOR таблица имеет следующую общую форму

$$XOR_\pi = \begin{vmatrix} 2^m & 0 & 0 & \cdots & 0 \\ 0 & a_{1,1} & a_{1,2} & \cdots & a_{1,2^{m-1}} \\ 0 & a_{2,1} & a_{2,2} & \cdots & a_{2,2^{m-1}} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & a_{2^{m-1},1} & a_{2^{m-1},2} & \cdots & a_{2^{m-1},2^{m-1}} \end{vmatrix} \overset{def}{=}$$

$$\overset{def}{=} \begin{vmatrix} 2^m & 0 \\ 0 & A_\pi \end{vmatrix}.$$

Мы будем интересоваться свойствами $2^{m-1} \times 2^{m-1}$ подматрицы $A_\pi = \left| a_{i,j} \right|$, $1 \le i, j \le 2^{m-1}$, которая соответствует части XOR таблицы с входами (ячейками), приписываемыми к ненулевым характеристикам.

Рассмотрим задачу определения вероятности события, заключающегося в том, что значение дифференциальной таблицы случайно взятой подстановки π порядка 2^m для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно $2k$ (значения ячеек XOR таблицы всегда четное). Как и в [5] эту вероятность обозначим $\Pr(\Lambda_\pi(\Delta X, \Delta Y) = 2k)$.

В [5] приводится теорема 2.1, определяющая эту вероятность в виде:

Утверждение. *Для любых ненулевых фиксированных ΔX, $\Delta Y \in Z_2^m$ в предположении, что подстановка π выбрана равновероятно из множества S_2^m и $0 \le k \le 2^{m-1}$,*

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)= \\ =\binom{2^{m-1}}{k}^2\cdot\frac{k!\cdot 2^k\cdot\Phi(2^{m-1}-k)}{2^m!}, \quad (1)$$

где функция $\Phi(d)$ определяется выражением

$$\Phi(d)=\sum_{i=0}^{d}(-1)^i\cdot\binom{d}{i}^2\cdot 2^i\cdot i!\cdot(2d-2i)!. \quad (2)$$

Как уже отмечалось выше, в [5] доказательства этих результатов приведены схематично (не полностью) и трудно понимаемы, а главное они не приведены к нужному нам виду. Мы здесь предлагаем более простую и более прозрачную версию доказательства этой и других теорем с последующей своей интерпретацией получающихся результатов.

Доказательство. Заметим сначала, что при операции вычисления разностей XOR входов подстановки π они попарно переходят друг в друга ($\Delta X = X\oplus X' = X'\oplus X$). Поэтому в дифференциальной таблице число переходов входной разности ΔX в выходную разность ΔY (значение ячейки таблицы дифференциальных разностей) всегда четное, и к тому же входы (и соответствующие выходы) подстановки распределяются по парам, так что для одной и той же разности ΔX мы имеем дело с 2^{m-1}-ой парами входов. Одновременно становится понятным, что для заданного сочетания входов и выходов подстановки π каждое конкретное значение входной разности может переходить не во все возможные значения выходных разностей, и что разные пары входов с одной и той же разностью ΔX могут переходить в одну и ту же выходную разность ΔY.

Для подстановок, выбираемых равновероятно из множества S_2^m, под искомой вероятностью, очевидно, следует понимать отношение числа подстановок $\pi\in S_2^m$, обладающих желаемым свойством (реализующих необходимое число $(2k)$ раз заданный переход $\Delta X\to\Delta Y$), к общему числу подстановок симметрической группы S_2^m:

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=\frac{\#\left\{\Lambda_\pi(\Delta X,\Delta Y)=2k\right\}}{2^m!}. \quad (3)$$

Выполним подсчет числа подстановок $\#\left\{\Lambda_\pi(\Delta X,\Delta Y)=2k\right\}$ с обусловленным количеством переходов входных разностей ΔX в выходную разность ΔY. Очевидно, что в это число будут входить подстановки, отличающиеся конфигурациями (сочетаниями) входов и выходов, участвующих в реализации желаемого свойства (реализующих необходимое число $(2k)$ раз заданный переход $\Delta X\to\Delta Y$).

Поскольку k пар переходов любой подстановки, участвующих в реализации необходимого свойства $\Delta X\to\Delta Y$, и $2^{m-1}-k$ оставшихся из общего числа 2^{m-1} пар переходов со свойством $\Delta X\to\Delta Y$ (обозначение из работы Эли Бихама и Ади Шамира [6]) компонуются в произвольном сочетании (переходы каждой из этих двух групп входов и выходов подстановки формируются независимо друг от друга), то интересующее нас число включает две компоненты (два сомножителя):

– первый сомножитель определяется числом различных подстановок π, у которых k пар входов из имеющегося в подстановке 2^{m-1} числа таких пар реализуют заданный переход $\Delta X\to\Delta Y$ (независимо от остальных $2^{m-1}-k$ пар входов каждой из подстановок);

– второй сомножитель определяется дополнительным расширением множества подстановок, у которых k пар входов реализуют заданный переход $\Delta X\to\Delta Y$, за счет многообразия вариантов выбора $2^{m-1}-k$ оставшихся пар входов каждой из подстановок, которые заданного перехода не реализуют, т.е. для которых $\Delta X\to\Delta Y$.

Рассчитаем сначала число вариантов подстановок, определяющих первый сомножитель.

Начнем с того, что в соответствии с комбинаторными соображениями для фиксированного набора из k пар входов, имеющих разность ΔX, которые имеют заданную выходную разность ΔY, возможно $k!$ вариантов различных перестановок k пар выходов по заданному набору входов (подстановки нормализованного вида отличаются расстановкой пар выходных значений по парам входных).

Очередной возможностью расширения множества подстановок, которые имеют заданное число k переходов входной разности ΔX в выходную разность ΔY, является варьирование наборами входов и выходов подстановки, участвующими в формировании переходов входной разности ΔX в выходную разность ΔY. Из общего числа 2^{m-1} пар входов, имеющих разность ΔX, в формировании интересующих нас переходов участвует только k пар входов. Очевидно, что они могут быть выбраны из общего числа 2^{m-1} пар входов $C_{2^{m-1}}^k$ способами. Аналогичное положение характерно и для множества пар выходов, имеющих разность ΔY. Поскольку компоновка входных и выходных пар осуществляется независимо, то приходим к общему числу $\left(C_{2^{m-1}}^k\right)^2$ вариантов подстановок с интересующим нас свойством.

Наконец, имеется еще одна степень свободы в построении подстановок с заданным числом переходов входной разности ΔX в выходную разность ΔY. Одна и та же пара входов с разностью ΔX может реализовать два варианта переходов в выходную разность ΔY (входы подстановки, входящие в пару, можно поменять местами). Но тогда множество возможных подстановок с фиксированным переходом входной разности ΔX в выходную разность ΔY дополнительно увеличится ещё в 2^k раз.

В результате мы действительно для вероятности того, что значение дифференциальной таблицы случайно взятой подстановки π порядка 2^m с переходом входной разности ΔX в соответствующую выходную разность ΔY будет равно числу $2k$, приходим к соотношению (1), в котором роль второго сомножителя, о котором шла речь выше, играет функция $\Phi(2^{m-1}-k)$.

Остается учесть варианты расширения множества подстановок интересующего нас вида за счет второго сомножителя. В работе [5], чтобы определить второй сомножитель, выводится расчетное соотношение для функции $\Phi(d)$ в виде соотношения (2).

Для получения этого расчетного соотношения в [5] использована «Спаривающая теорема», краткое доказательство которой без разъяснений, приводит автор. Мы здесь предлагаем свой вариант вывода расчетного соотношения для функции $\Phi(d)$, являющегося по существу следствием доказанного выше соотношения (1).

Действительно, будем теперь интересоваться «хвостом» из $2^{m-1}-k$ пар входов и выходов, которые в предыдущем рассмотрении не учитывались (считались фиксированными). По оговоренному условию это пары, которые не имеют заданного перехода $\Delta X \to \Delta Y$. Множество этих пар можно рассматривать как отдельную подстановку порядка 2^m-2k. Тогда для определения числа подстановок порядка 2^m-2k, не имеющих заданного перехода $\Delta X \to \Delta Y$, очевидно можно просто из общего числа подстановок такого порядка вычесть число подстановок, имеющих заданный переход. Подстановки порядка 2^m-2k с обусловленным переходом могут содержать одну пару с таким переходом, две пары, и так до 2^m-2k пар переходов.

В результате в терминах функции $\Phi(d)$ выражение для расчета второго сомножителя можно представить в виде

$$\Phi(d)=(2d)!-\sum_{i=1}^{d} i!\cdot 2^i\binom{d}{i}^2\Phi(d-i). \qquad (4)$$

Остается показать, что представления (2) и (4) эквивалентны.

Это легко устанавливается последовательной подстановкой в (4) значений функции $\Phi(d-i)$, $i=1,2,\ldots,d$ и использованием очевидных соотношений

$$1!\cdot 2^1\cdot\binom{d}{1}^2\cdot 1!\cdot 2^1\cdot\binom{d-1}{1}^2-2!\cdot 2^1\cdot\binom{d}{2}^2=$$

$$=2!\cdot 2^2\cdot\binom{d}{2}^2$$

для коэффициента при функции $\Phi(d-2)$ после подстановки в (4) явного вида функции $\Phi(d-1)$;

$$-\left[1!\cdot 2^1\cdot\binom{d}{1}^2\cdot 1!\cdot 2^1\cdot\binom{d-1}{1}^2-2!\cdot 2^2\cdot\binom{d}{2}^2\right]\times$$

$$\times\left[1!\cdot 2^1\cdot\binom{d-2}{1}^2\right]+$$

$$+\left[1!\cdot 2^1\cdot\binom{d}{1}^2\cdot 2!\cdot 2^2\cdot\binom{d-1}{2}^2-3!\cdot 2^3\cdot\binom{d}{3}^2\right]=$$

$$=-3!\cdot 2^3\cdot\binom{d}{3}^2$$

для коэффициента при функции $\Phi(d-3)$ после подстановки в (4) явного вида функции $\Phi(d-2)$ и так до свертывания коэффициентов при всех последующих функциях $\Phi(d-i)$, $i=4,5,\ldots,d$. В результате приходим к выражению (2). Утверждение доказано.

Далее, как и в [5] обозначим ожидаемое число ненулевых характеристик ΔX, ΔY, для которых $\Lambda_\pi(\Delta X,\Delta Y)=2k$ как $\Lambda_{m,2k}$.

При выводе выражения (1) мы не фиксировали значений пары разностей $\Delta X, \Delta Y \in Z_2^m$, для которых оно получено. Это значит, что соотношение (1) справедливо для произвольных сочетаний разностей на входе и выходе подстановок. Мы уже отмечали ранее, что результаты, полученные для ансамбля подстановок, считаются справедливыми и для отдельной подстановки π, т.е. полученные формулы можно трактовать как закон распределения ненулевых характеристик для каждой подстановки.

Выражение (1) определяет вероятность того, что в XOR таблице случайно взятой подстановке число переходов входной разности $\Delta X \in Z_2^m$ в выходную разность $\Delta Y \in Z_2^m$ будет равно $2k$.

Но тогда становится понятным, что выражение для числа $\Lambda_{m,2k}$ переходов таблицы дифференциальных разностей подстановки порядка 2^m обусловленного типа, – а именно для среднего значения числа ненулевых характеристик $\Delta X \to \Delta Y$, таких, что $\Lambda_\pi(\Delta X,\Delta Y)=2k$, – может быть получено путем умножения выражения (1) на число ячеек подматрицы $A_\pi=\left|a_{i,j}\right|$ таблицы XOR_π равное $(2^m-1)^2$:

$$\Lambda_{m,2k}=\frac{(2^m-1)^2}{2^m!}\cdot\binom{2^{m-1}}{k}^2\cdot k!\cdot 2^k\cdot\Phi(2^{m-1}-k). \qquad (6)$$

Это выражение и есть то, которое нам нужно.

2. СРАВНЕНИЕ РАСЧЕТНЫХ И ЭКСПЕРИМЕНТАЛЬНЫХ РЕЗУЛЬТАТОВ

Нас теперь будет интересовать среднее значение максимума таблицы XOR разностей. Оно находится из соотношения (6) просто путем определения максимального значения k, при котором результат расчетов по этому выражению при-

водит к наименьшему целому значению. Другими словами, нам нужно найти решение уравнения

$$\frac{(2^m-1)^2}{2^m!}\cdot\left(\begin{array}{c}2^{m-1}\\ k\end{array}\right)^2\cdot k!\cdot 2^k\cdot\Phi(2^{m-1}-k)\approx 1. \qquad (7)$$

Это решение можно искать переборным методом, ориентируясь при этом на экспериментальные данные.

Полезной аппроксимацией для выполнения расчетов может стать и еще один результат, также приведенный в работе [5]. Имеется в виду замечание о том, что в знакопеременной сумме в выражении (2) первый терм (при $i=0$) является доминирующим, и что

$$\Phi(d)\approx(2d)!/e^{\frac{1}{2}}.$$

Остается заметить, что $e^{-\frac{1}{2}}=0{,}6065$.

Например, для $m=4$, $k=3$ получим

$$\Lambda_{4,6}=\frac{(2^4-1)^2}{2^4!}\cdot\left(\begin{array}{c}2^{4-1}\\ 3\end{array}\right)^2\cdot 3!\cdot 2^3\cdot\Phi(2^{4-1}-3).$$

С учетом того, что $\Phi(5)=2088960$ в итоге приходим к результату

$$\Lambda_{4,6}=\frac{15^2}{2^4!}56^2\cdot 3!\cdot 2^3\cdot 2088960=3{,}379.$$

Мы получили ожидаемое среднее значение максимума таблицы дифференциальных разностей для значения $m=4$ несколько большее $2k=6$, что хорошо согласуется с результатами наших экспериментов.

Для других значений m расчеты, выполненные в соответствии с соотношениями (1), (2) и (7), представлены в табл. 1.

Таблица 1

Сравнение расчетных и экспериментальных результатов

m	$\Lambda_\pi(\Delta X,\Delta Y)=2k$	$2k$	Эксперимент
4	3,379 0,459	6 8	6,7 $\le(m+3)$
5	3,08 1,708	6 8	7,94 $\le(m+3)$
6	6,6 0,675	8 10	9,1 $\le(m+4)$
7	2,641 0,221	10 12	10,3 $\le(m+4)$
8	0,8748	12	11,4
9	3,474 0,248	12 14	12,5 $\le(m+4)$
10	13,8495 0,99	12 14	13,4 $\le(m+4)$
11	3,952 0,247	14 16	14,5 $\le(m+4)$
12	15,787 0,987	14 16	15,3 $\le(m+4)$

Таблица 2 иллюстрирует результаты вычислительного эксперимента, полученные нами ра-

Таблица 2

Результаты вычислительного эксперимента

Степень подстановки / Число циклов подстановки	23 = 8	24 = 16	25 = 32	26 = 64	27 = 128	28 = 256	29 = 512	210 = 1024	211 = 2048	212 = 4096
1	4.8014	6.69454	7.94398	9.11202	10.2827	11.4222	12.0	13.75	15.3333	14.0
2	4.2591	6.71003	7.94526	9.11991	10.2921	11.3765	12.3467	13.6429	14.1538	15.0
3	4.7807	6.68965	7.94006	9.11311	10.3022	11.4241	12.3697	13.2647	14.3947	15.68
4	4.2616	6.71753	7.94177	9.11112	10.3097	11.3012	12.5144	13.4481	14.5745	15.3235
5	4.9487	6.6881	7.94223	9.10677	10.3043	11.3252	12.4528	13.4565	14.3969	15.4066
6	4.5187	6.71281	7.95425	9.11403	10.3178	11.3645	12.4948	13.3743	14.529	15.3509
7	8.0	6.72067	7.94278	9.11009	10.3157	11.3144	12.4095	13.4121	14.3967	15.37
8	8.0	6.84496	7.94878	9.11502	10.3248	11.3216	12.4316	13.4607	14.5284	15.4055
9		7.0137	7.95743	9.11899	10.3165	11.2887	12.4122	13.3596	14.5089	15.4027
10		6.91892	7.98563	9.1015	10.3071	11.3538	12.5669	13.4009	14.4336	15.4268
11		8.0	8.03191	9.15496	10.3183	11.359	12.4249	13.3284	14.4715	15.368
12			7.6	9.0	10.2954	11.3429	12.3457	13.2179	14.4822	15.3313
13			8.0	9.42222	10.2264	11.0667	12.7111	13.55	14.4785	15.2735
14				9.0	10.5882	11.0	12.7619	13.125	14.3939	15.625
15				10.0	9.33333	11.0	12.0	13.4667	14.1935	15.4333
16					10.0	12.0	12.0	13.5	14.4	15.5333
17					10.0			13.0	14.0	15.7143
18								14.0	14.05.09	15.6
19									-	16.5
Число подстановок	1000000	1000000	1000000	500000	100000	10000	5000	5000	5000	5000

нее и приведенные в работе [1] (здесь они даны в более полном объеме).

Расчеты, выполненные в соответствии с выражением (6), для 16-битной подстановки представлены также в левой колонке табл. 3. В правой колонке этой таблицы представлены соответствующие результаты для 16-битного шифра по Хейсу [7] с линейным преобразованием, подобным операции MixColumn в шифре Rijendael.

Таблица 3

Распределение парных разностей для SPN шифра с умножением на матрицу

Расчет		Эксперимент	
#2.	1302484861	#2.	1302551726
#4.	325626184	#4.	325625709
#6.	54271858	#6.	54253870
#8.	6784085	#8.	6781574
#10.	678418	#10.	677785
#12	56535	#12	56793
#14.	4038	#14.	3974
#16.	252	#16.	272
#18.	14	#18.	17
#20.	1	#20.	0

Сопоставление результатов таблиц 1 и 2, а также таблицы 3 свидетельствует о хорошем согласовании полученных ранее и следующих из теоретических рассуждений результатов.

Интересно отметить, что для закона распределения (1) с большой точностью выполняется соотношение

$$\sum_{k=0}^{k^*}(2^{m-1}-1)^2\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=\left(2^{m-1}\right)^2-2^m,$$

и, следовательно, справедливо равенство

$$\sum_{k=0}^{k^*}\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=\frac{\left(2^{m-1}\right)^2-2^m}{(2^{m-1}-1)^2}.$$

В свою очередь легко убедиться, что

$$\frac{\left(2^{m-1}\right)^2-2^m}{(2^{m-1}-1)^2}=\frac{2^{m-1}\cdot\left(2^{m-1}-2\right)}{(2^{m-1}-1)^2}=$$

$$=\frac{1}{1-2^{-m+1}}\cdot\frac{1-2^{-m+2}}{1-2^{-m+1}}\approx 1.$$

Это означает, что для выражения (1) с большой точностью выполняется условие нормировки

$$\sum_{k=0}^{k^*}\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=1.$$

Здесь k^* представляет собой половину от максимального значения числа переходов XOR таблицы случайной подстановки.

Таким образом, формула (1) может рассматриваться как закон распределения числа ненулевых (по входу) переходов $\Delta X\to\Delta Y$ для отдельной подстановки, т.е. набор значений переходов $\Lambda_\pi(\Delta X,\Delta Y)=2k$, $k=0,1,\ldots,k^*$ представляет практически полную группу событий. Мы фактически и воспользовались этим, выполняя вычисления по выражению (6).

В табл. 4 представлены результаты вычисления значений «хвостов» формулы (1), т.е. $\sum_{k=k^*+1}^{2^{m-1}}\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$ как функции размера битового входа подстановки m (в скобках представлены значения этих же сумм «хвостов», умноженных на число ячеек подматрицы A_π XOR таблицы). Видно, что даже в «нормированном» варианте доля сумм «хвостов» оказывается незначительной.

Таблица 4

Результаты расчетов хвостов распределений

m	k^*	$\sum_{k=k^*+1}^{2^{m-1}}\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$
4	3	0,00245 (0,55)
6	5	0,000015 (0,06)
8	6	0,000001 (0,065)
10	7	0,00000006 (0,062)
12	8	0,0000000034 (0,0057)

Этим подтверждается высказанная в начале статьи установка, что свойства отдельной случайной подстановки однозначно выражаются через свойства ансамбля случайных подстановок.

Вместе с тем, мы хотим еще раз обратить здесь внимание читателей на то, что отмеченные выше результаты характерны не только для случайных подстановок, но и для многоцикловых шифрующих преобразований, свойственных блочным симметричным шифрам вообще. Наши эксперименты показывают, что шифрующее преобразование (любой современный шифр) асимптотически (для Rijndael подобных шифров уже после 4-х циклов) для различных ключей зашифрования ведет себя как случайная подстановка, т.е. и для него оказываются справедливыми расчетные соотношения, представленные в этой работе.

Соответствующие идеи в этом направлении высказываются и в цитируемой нами работе [5]. Однако Luka O'Connor связывает свои результаты только с шифрами, использующими случайные подстановки, и как во многих известных работах, посвященных оценке стойкости БСШ к атакам дифференциального криптоанализа, показатели стойкости шифров связываются с дифференциальными свойствами подстановочных преобразований, использованных при их построении. Полученные нами с использованием уменьшенных моделей шифров Rijndael, Камелия, а также шифров Мухомор, Лабиринт, Калина и ADE, представленных на Украинский конкурс по выбору национального стандарта блочного симметричного шифрования, а также ряда других шифров, экспериментальные результаты свидетельствуют о том, что реальные

асимптотические (при полных наборах цикловых преобразований) значения максимальных и средних вероятностей дифференциальных и линейных характеристик (полных дифференциалов и линейных корпусов) для этих шифров являются свойством, не зависящим ни от свойств S-блоков, ни от числа циклов (после определенного их числа), ни от способа введения в цикловые функции подключей [3]. Они определяются, как уже было отмечено выше, свойствами шифрующего преобразования именно как случайной подстановки, несмотря даже на то, что БСШ реализует существенно меньшую часть всего множества подстановок соответствующего порядка. А это означает, что на основе полученных в работе соотношений действительно может строиться методика оценки стойкости шифров к атакам дифференциального криптоанализа.

Мы здесь в определенном смысле повторяем рассуждения Luka O'Connor-а, но в более корректной, как нам кажется, форме (некоторые рассуждения и соотношения раздела в [5], посвященного формированию оценок стойкости к атакам дифференциального криптоанализа, нам представляются не совсем корректными).

Luka O'Connor, поднимая вопрос о связи дифференциальных показателей случайных подстановок с устойчивостью к атакам дифференциального криптоанализа, рассматривает отображение G, базирующееся на m-битных подстановках выбранных равновероятно из S_{2^m}. Отображение G, в частности, считается состоящим из S-блоков, являющихся m-битными подстановками $\pi_1, \pi_2, \ldots, \pi_s$ такими, что $G: Z_2^{m \cdot s} \to Z_2^{m \cdot s}$, где π_1 – первый блок из s битов, π_2 операция второго блока из s битов и т.д. Далее он говорит о вероятности самой вероятной характеристики (probability of the most likely characteristic), покрывающей весь шифр, выражая ее через соответствующую вероятность одноцикловой характеристики p^{Ω}. Он считает, что для любой r-цикловой характеристики выполняется условие $p^{\Omega_r} \le \left(\frac{\Lambda_m^*}{2^{m-1}} \right)^r$, где Λ_m^* определяется соотношением

$$2^m p^{\Omega} \le \Lambda_m^* \stackrel{def}{=} \max_{\substack{\pi \in (\pi_1, \pi_2, \ldots, \pi_s) \\ \Delta X, \Delta Y \in Z_2^m \\ w(\Delta X), w(\Delta Y) > 0}} \Lambda_\pi(\Delta X, \Delta Y).$$

И если с понятием и определением самой вероятной характеристики можно согласиться, то дальнейшее рассмотрение задачи определения общей границы для значения самой вероятной характеристики нам представляется не совсем аккуратным (хотя бы из-за того, что вероятности входят в неравенства равноправно с числом ненулевых характеристик: $\Pr(\Lambda_m^* = 2k) < \Pr(\Lambda_\pi = 2k) \le \Lambda_{m,2k}$, где $\Lambda_{m,2k}$ определяется формулой (6)). Тем не менее, окончательный результат, сформированный Luka O'Connor-ом в виде Утверждения 3.1, о том, что для больших m и предположении равномерного распределения подстановок на множестве S_{2^m} ожидаемая вероятность самой правдоподобной (вероятной) ненулевой дифференциальной характеристики ограничена значением $\frac{m}{2^{m-1}}$, оказывается, как мы увидим далее, близким к истине. Однако это утверждение строится Luka O'Connor-ом на результатах, полученных эмпирическим путем, и никак не связано со свойствами шифрующих преобразований.

Наша позиция состоит в том, что результирующие дифференциальные свойства блочных симметричных шифров (по крайней мере, Rijendael-подобных шифров) не связаны со свойствами S-блоков шифра, а являются общим свойством шифра как случайной подстановки. Особенностью шифрующего преобразования в виде БСШ, рассматриваемого как подстановка, является существенно меньшее множество реализуемых им подстановок. БСШ реализует только 2^m (по числу ключей) подстановок из общего их числа $2^m!$, причем, несмотря на такое существенное уменьшение допустимого множества подстановок, оно продолжает сохранять свойства, характерные для множества случайных подстановок [3, 4, 9] (по инверсиям, возрастаниям, циклам, дифференциальным и линейным характеристикам).

И если, определяя среднее значение максимума таблицы дифференциальной разности (полного дифференциала шифра-подстановки) для произвольной случайной подстановки, мы можем говорить о том, что существует, хотя и очень мало вероятное, значение максимума, превышающее (может быть даже существенно) среднее значение максимума, то для шифра таких мало вероятных значений, сколько-нибудь заметно отличающихся от среднего значения максимума нет. Наши эксперименты с малыми моделями шифров показывают, что среднее значение максимума для полного дифференциала шифра практически как раз и является наиболее вероятным (граничным) значением.

Опираясь на экспериментальные данные, для определения реальной границы максимума полного дифференциала (таблицы XOR разностей для всего шифра), можно рассмотреть отношение $\frac{\Lambda_{m,2k}}{k}$, из которого можно определить граничное значение k, при котором оно становится меньшим единице. Полученное значение k_{max} и следует принять в качестве максимально вероятного значения дифференциала. Но именно эта задача и решалась при построении таблицы 1. Как следует из данных расчетов и экспериментов, максимально возможное значение дифференциала для подстановки порядка 2^m оказывается близким к $m + 4$, что укладывается в границы, оговоренные Luka O'Connor-ом, и, следовательно, утверждение 3.1 из работы [5], опираясь на наши эмпирические

данные, применительно к блочным симметричным шифрам (что выходит за рамки, оговоренные Luka O'Connor-ом) можно перефразировать так:

Утверждение. *Для шифрующих преобразований, определяемых многоцикловыми процедурами перестановочно-подстановочных биективных отображений, свойственными современным блочным симметричным шифрам, ожидаемая вероятность самой правдоподобной ненулевой дифференциальной характеристики ограничена значением* $\frac{m+4}{2^m}$.

Таким образом, дифференциальные свойства шифрующих преобразований современных блочных симметричных шифров (при заявленном числе циклов преобразования) являются одним из проявлений свойств случайных подстановок, и в этом смысле шифр Rijendael и шифры, представленные на Украинский конкурс, являются эквивалентными (неразличимыми). Все они реализуют наибольшую вероятность максимума полного дифференциала (для 128 битных версий) близкую к 2^{-120}. Кстати, эти же характеристики стойкости к атакам дифференциального криптоанализа демонстрирует при соответствующем числе циклов (например, при 10 как в шифре Rijendael) и классическая SPN структура, рассмотренная в 1973 г. в работе Х. Фейстеля [8] (16-битная конструкция этого типа детально исследована проф. Н. Хеусом [7]).

На основе полученных результатов можно, тем не менее, предложить подход к сравнению эффективности решений по построению алгоритмов шифрования (при прочих равных условиях) в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума полных дифференциалов.

По этому показателю, как свидетельствует анализ уменьшенных версий рассмотренных шифров, преимущество следует отдать шифру Лабиринт, который выходит на асимптотическое значение показателя уже при двух итерациях (за счет мощного начального преобразования), далее следует Rijendael и решения, представленные на украинский конкурс (4-е цикла), и затем уже идет SPN шифр Х. Фейстеля (6-ть циклов).

Другой важный вывод, который напрашивается по результатам экспериментов, состоит в том, что при мощном (доцикловом) преобразовании и другие известные решения по построению блочных шифров, в том числе и обобщенная SPN структура Х. Фейстеля (с существенно худшим по эффективности чем примененное в шифре Rijendael линейным преобразованием) обеспечивает дифференциальные свойства (максимальную вероятность полного дифференциала), не уступающие шифру Rijendael и по скорости достижения асимптотических показателей. Использование в таких структурах случайных S-блоков обеспечит и повышенную по сравнению с шифром Rijendael устойчивость к алгебраическим атакам.

Литература

[1] *Олейников Р. В., Лисицкий К. Е.* Исследование дифференциальных свойств подстановок различных цикловых классов. Двенадцатая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах», 19-20 МАЯ 2009 г., Тезисы докладов. – К.: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ", 2009. – С. 24-25.

[2] *Олейников Р.В., Лисицкая И.В., Широков А.В., Лисицкий К.Е.* Исследование дифференциальных свойств подстановок. Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. I, С. 59-63.

[3] *Долгов В.И., Лисицкая И.В., Олешко О.И., Золочевская А.Ю., Дроботько Е.В.* К вопросу оценки стойкости БСШ к атакам линейного и дифференциального криптоанализа. Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. II, С. 35-39.

[4] *Долгов В.И., Лисицкая И.В., Киянчук Р.И.* Rijndael – это новое или хорошо забытое старое? Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. II, С. 32-35.

[5] *L. J. O'Connor.* On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, vol. 795, T. Helleseth ed., Springer-Verlag, pages 360-370, 1994.

[6] *E. Biham and A. Shamir.* Differential cryptanalysis of the full 16-round DES. Technical Report 708. Technion, Israel Institute of Technology, Haifa, 1991.

[7] *H.M. Heys.* A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v. 26, N 3, 2002, p. 189-221.

[8] *H. Feistel,* Cryptography and computer privacy. Scientific American, 228(5): 15-23,1973.

[9] *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. – Т. 6, № 2 – С. 257-263.

Поступила в редколлегию 25.06.2010.

Олейников Роман Васильевич, кандидат технических наук, докторант кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

Олешко Олег Иванович, старший преподаватель кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

Лисицкий Константин Евгеньевич, студент 1-го курса кафедры БИТ ХНУРЭ. Область научных интересов: криптографическая защита информации.

Тевяшев Андрей Дмитриевич, доктор технических наук, профессор, заведующий кафедрой прикладной математики. Область научных интересов: криптографическая защита информации.

УДК 621. 391:519.2:519.7

Диференційні властивості підстановок / Р.В. Олійников, О.І. Олешко, К.Є. Лисицький, А.Д. Тевяшев // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 326-333.

Виводяться розрахункові відношення для визначення середнього значення максимумів XOR таблиць випадкових підстановок. Показується. що диференційні властивості сучасних блокових симетричних шифрів (при заявленому числі циклів перетворення) являються одним із проявів властивостей випадкових підстановок. Пропонується підхід до порівняння ефективності рішень по побудові алгоритмів шифрування у вигляді мінімальної кількості циклів алгоритму, при якій реалізується асимптотичний показник середнього значення максимуму повних диференціалів.

Ключові слова: симетричний блоковий шифр, диференційний криптоаналіз, випадкова перестановка.

Табл. 04. Бібліогр.: 09 найм.

UDC 621. 391:519.2:519.7

Differential properties of substitutions / R.V. Oleinykov, O.I. Oleshko, K.E. Lisitskiy, A.D. Tevyashev // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 326-333.

Computational relations for determining the overage of maximum values of XOR tables of random substitutions are derived. It is shown that differential properties of present-day block symmetric ciphers (with the declared number of transformation cycles) are one of the manifestations of properties of random substitutions. An approach to comparing the efficiency of solutions on construction of encryption algorithms in the form of a minimum number of cycles of an algorithm is suggested, which implements an asymptotic index of the average maximum value of full differentials.

Key words: symmetric block cipher, differential cryptanalysis, random substitution.

Tab. 04. Ref.: 09 items.

УДК 621. 391:519.2:519.7

СВОЙСТВА ТАБЛИЦ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ СЛУЧАЙНЫХ ПОДСТАНОВОК

В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, О.И. ОЛЕШКО

Выводятся расчетные соотношения для среднего значения максимумов таблиц линейных аппроксимаций случайных подстановок. Показывается, что линейные свойства шифрующих преобразований современных блочных симметричных шифров (при заявленном числе циклов преобразования) являются одним из проявлений свойств случайных подстановок. Предлагается подход к сравнению эффективности решений по построению алгоритмов шифрования в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума линейного корпуса.

Ключевые слова: линейные аппроксимации, случайные подстановки.

ВВЕДЕНИЕ

Интерес и внимание к исследованию и разработке процедур генерации криптографически стойких S-блоков возник в начале 90-х годов прошедшего столетия [1, 2, 3, 4, 5, 6 и др.]. Он стал закономерным исходом изучения и исследования специалистами надежности американского стандарта симметричного шифрования DES, завоевавшим к тому времени мировой авторитет и признание (ставшим фактически всемирным стандартом). К этому же времени относится появление работы израильских ученых-криптографов Бихама и Шамира [7], предложивших атаку дифференциального криптоанализа на шифр DES, а двумя годами позже работы Мацуи [8], посвященной линейному криптоанализу – второму новому типу криптонападения на DES. Эти работы стали заметным стимулом дальнейшего разворачивания работ, посвященных исследованию и анализу S-блоковых конструкций и алгоритмов [9-16 и мн. другие], может быть часто не опирающиеся прямо на S-блоковые конструкции, но, тем не менее, имеющие к ним самое непосредственное отношение. Сегодня эти работы, конечно уже вышли далеко за рамки шифра DES. Появилось множество новых решений по построению алгоритмов шифрования. На смену самого шифра DES в США не так уж и давно принят новый стандарт шифрования AES (FIPS-197). Естественно, что параллельно с развитием техники конструирования шифров происходило и совершенствование методов криптоанализа, направленных на преодоление показателей стойкости, закладываемых в шифр его разработчиками. Это значит, что и сегодня вопросы построения более совершенных процедур шифрования и алгоритмов криптографической защиты информации в целом не потеряли своей актуальности, а, следовательно, в центре внимания криптографов и математиков продолжают оставаться методы и алгоритмы конструирования новых шифров и в том числе методы (генерации) более совершенных S-блоковых конструкций.

Мы хотим здесь обратить внимание читателей на то, что многие исследователи связывают показатели стойкости шифров к атакам дифференциального и линейного криптоанализа с соответствующими показателями S-блоков, с помощью которых осуществляются нелинейные преобразования во многих шифрах. Так, в работах [17,18 и др.] результирующие показатели стойкости шифров к указанным атакам напрямую выражаются через значения максимумов таблиц XOR разностей и линейных аппроксимаций входящих в шифр S-блоковых преобразований. Наши эксперименты с малыми версиями шифров, однако, показывают, что асимптотические характеристики устойчивости шифров не совпадают с показателями, определяемыми через максимумы таблиц XOR разностей или соответственно максимумы таблиц линейных аппроксимаций подстановочных конструкций. Более того, наши эксперименты с уменьшенными копиями современных шифров показывают, что их асимптотические характеристики вообще не зависят от максимумов таблиц XOR разностей и таблиц линейных аппроксимаций используемых в шифрах S-блоков.

Здесь мы продолжаем исследования, начатые в нашей работе [19], где мы рассматривали свойства таблиц XOR разностей случайных подстановок. Теперь мы будем интересоваться свойствами таблиц линейных аппроксимаций случайных подстановок. В этой работе ставится задача получить распределение значений ячеек таблиц линейных аппроксимаций S-блоков расчетным путем.

1. ЗАКОН РАСПРЕДЕЛЕНИЯ СМЕЩЕНИЙ ТАБЛИЦ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ СЛУЧАЙНЫХ ПОДСТАНОВОК

Отметим, что и в этом случае (имеется в виду наша работа [19]), близкую по постановке задачу нам удалось найти также в работах Luka O'Connora [20, 21] 1995-го года, в которых приводятся интересующие нас расчетные соотношения без доказательств. Кроме того, нас не удовлетворила и авторская интерпретация конечных результатов, что определило целесообразность изложения собственной позиции по этому вопросу.

И в этой работе мы воспользуемся центральной идеей развиваемого в [20, 21] подхода, а именно будем считать, что свойства отдельной

случайной подстановки однозначно выражаются через свойства ансамбля случайных подстановок, и на этой основе представим свою версию доказательств и интерпретации соответствующих результатов.

Далее рассматриваются подстановки общего вида порядка 2^n, к которым можно отнести и шифрующие преобразования, осуществляемые для каждого n-битного блока данных P и фиксированного значения ключа K симметричными шифрами. Заметим, однако, сразу, что множество подстановок (с операцией умножения подстановок) в классическом понимании образуют симметрическую группу, обозначаемую в математической литературе как S_2^n, порядок которой равен $2^n!$, в то время как множество подстановок, образуемое симметричными шифрами, не является группой и их число ограничено значением 2^n (числом ключей).

В линейном криптоанализе интересуются значениями (входами) в так называемые линейные аппроксимационные таблицы (LAT) S-блоков, которые, как отмечается в [20, 21], после вычитания нормировочного значения 2^{n-1} представляют собой корреляции линейных комбинаций с входами и выходами S-блоков.

Напомним ряд определений.

Следуя работе [21], пусть $\pi: Z_2^n \to Z_2^n$ – биективное n-битное отображение и пусть S_2^n будет множеством всех таких отображений. Для n-битного вектора $X \in Z_2^n$ пусть X_i обозначает i-тый бит вектора X. Линейная аппроксимационная таблица для подстановки p обозначается LAT_π и является таблицей размера $2^n \times 2^n$ с элементами $LAT_\pi(\alpha,\beta)$, определяемыми соотношением

$$LAT_\pi(\alpha,\beta) \stackrel{def}{=}$$

$$\stackrel{def}{=} \#\left\{ X / X \in Z_2^n, \stackrel{n}{\oplus}_{i=1} X[i]\cdot\alpha[i] = \stackrel{n}{\oplus}_{i=1} \pi(X[i])\cdot\beta[i] \right\},$$

где $\alpha,\beta \in Z_2^n$ и $'\cdot'$ обозначает операцию побитного логического ИЛИ.

В соответствии с приведенным определением, $LAT_\pi(\alpha,\beta)$ представляет собой число равенств четности между линейной комбинацией входных битов (определяемых маской α по входу в LAT_π подстановки по строкам) и линейной комбинацией выходных битов (определяемых маской β по входу в таблицу LAT_π подстановки по столбцам).

Нас будет интересовать теорема, которая приведена в работе [20] без доказательства.

Теорема 1: *Пусть* $\lambda(\alpha,\beta)$ *будет случайным числом, соответствующим значению линейной аппроксимационной таблицы подстановки* $LAT_\pi(\alpha,\beta)$, *когда подстановка p выбрана равновероятно из множества* S_2^n *и маски* α,β *ненулевые. Тогда* $\lambda(\alpha,\beta)$ *для целых значений* k, $0 \le k \le 2^{n-1}$ *принимает только четные значения и вероятность, что* $\lambda(\alpha,\beta) = 2k$ *определяется выражением*

$$Pr\left(\lambda(\alpha,\beta) = 2k\right) = \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \left(\begin{array}{c} 2^{n-1} \\ k \end{array} \right)^2. \qquad (1)$$

Мы далее здесь предлагаем свой вариант ее доказательства.

Доказательство. Нас интересует число подстановок из общего их числа $2^n!$, ячейки таблиц $LAT_\pi(\alpha,\beta)$ которых для заданного значения входа в таблицы по строкам α и заданного значения входа в таблицы по столбцам β (заданного сочетания пары входов в LAT_π) имеют заполнением (значением) число $2k$.

По определению, если подстановка p имеет значение ячейки $LAT_\pi(\alpha,\beta)$ равное $\lambda(\alpha,\beta) = 2k$, то это означает, что число плайнтекстов P из общего их числа 2^n, прошедших при построении таблицы маску α с признаками чет и нечет (имеющих результатом скалярного произведения $\alpha \cdot P$ ноль или единицу), совпадающих с числом соответствующих шифртекстов C, прошедших маску β с признаками чет и нечет, равно $2k$ (число плайнтекстов, удовлетворяющих равенству четности $\alpha \cdot P = \beta \cdot C$, равно $2k$).

Итак, интересующее нас событие связано с совпадением признаков чет или нечет для плайнтекстов и шифртекстов, прошедших соответствующие маски.

Обратим в связи с этим внимание на то, что для любого из вариантов сочетаний масок $\alpha,\beta \in Z_2^n$ скалярные произведения $\alpha \cdot P$ также как и $\beta \cdot C$ формируются с использованием всех 2^n n-битных возможных значения входов и выходов. Причем ровно половина (2^{n-1}) из общего числа скалярных произведений для всего множества плайнтекстов (как и для всего множества шифртекстов) принимают значения "чет", а остальные 2^{n-1} скалярных произведений принимают значения "нечет". В результате различные подстановки при вычислении $LAT_\pi(\alpha,\beta)$ практически будут отличаться только распределением четных и нечетных значений множеств скалярных произведений $\alpha \cdot P$ и $\beta \cdot C$ из одного и того же набора (включающего 2^{n-1} четных и 2^{n-1} нечетных значений этих произведений).

Это означает, что каждая пара α и β значений масок для входов (по строкам и столбцам) в таблицы LAT_π при переборе по всем возможным значениям входов P в подстановку (при вариации по всем значениям плайнтекстов) будет приводить к одному и тому же закону распределения вероятностей параметра $\lambda(\alpha,\beta)$ – числа выполнения линейных соотношений $\alpha \cdot P = \beta \cdot C$ независимо от конкретных значений масок α и β.

Результирующее число "проходов" (выполнений равенства $\alpha \cdot P = \beta \cdot C$ для пары α и β будет определяться числом совпадений четов или нечетов в "списках" соответствующих наборов скалярных произведений, причем одно и то же значение числа "проходов" будут иметь подстановки, которые отличаются переходами (перестановками), сохраняющими четность (нечетность) компонент,

формирующих значение $\lambda(\alpha,\beta)$. Напомним, что параметр $\lambda(\alpha,\beta)$ фиксирует число случаев выполнения равенства $\alpha \cdot P = \beta \cdot C$ для каждой подстановки.

Докажем сначала дополнительное утверждение.

Утверждение 1. *Две последовательности, составленные из четного 2^n числа двоичных элементов, содержащие одинаковое число 2^{n-1} символов каждого типа, имеют только четное число совпадений* (*несовпадений*).

Доказательство. Пусть $\xi = \{0,1\}^n$ и $\zeta = \{0,1\}^n$ – две случайно взятые 2^n-битные последовательности с одинаковым числом нулей и единиц.

Доказательство будем вести от противного. Предположим, что последовательности ξ и ζ имеют нечетное число совпадений. Пусть для конкретности совпадающие символы имеют четное число нулей и нечетное число единиц. Тогда оставшиеся (несовпадающие) символы последовательностей для одной из них будут иметь нечетное число нулей и четное число единиц, в то время как вторая последовательность тогда должна иметь четное число нулей и нечетное число единиц (ведь они противоположные). В результате получается, что в одной последовательности должно быть четное число нулей и четное число единиц, в то время как во второй должно быть нечетное число нулей и нечетное число единиц, а это противоречит исходному предположению, что обе последовательности состоят из одинакового четного числа нулей и четного числа единиц. Следовательно, наше предположение о том, что последовательности ξ и ζ могут иметь нечетное число совпадений, не верно.

Из доказанного следует справедливость утверждения первой части теоремы о том, что параметр $\lambda(\alpha,\beta)$ линейных аппроксимационных таблиц подстановок принимает только четные значения, так как наборы признаков чет и нечет скалярных произведений можно интерпретировать как соответствующие двоичные последовательности.

Справедливо также и такое утверждение.

Утверждение 2. *Для двух последовательностей, составленных из четного 2^n числа двоичных элементов и содержащих одинаковое число 2^{n-1} символов каждого типа, совпадающие* (*несовпадающие*) *последовательности символов содержат одинаковое число единиц и нулей.*

Доказательство. Пусть $\xi = \{0,1\}^n$ и $\zeta = \{0,1\}^n$ – две случайно взятые 2^n-битные последовательности с одинаковым числом нулей и единиц и пусть $2k = s + t$, $s \neq t$ будет числом совпадающих символов (снова доказательство ведется от противного). Пусть далее для конкретности совпадающие символы содержат s единиц и t нулей. Тогда несовпадающие символы каждой из последовательностей ξ и ζ должны содержать $2^{n-1} - s$ единиц и $2^{n-1} - t$ нулей, причем $2^{n-1} - s \neq 2^{n-1} - t$ (разное число нулей и единиц). Но одинаковые наборы из нулей и единиц в ″хвостах″ каждой из последовательностей могут дать $2^{n-1} - 2k$ несовпадений только тогда, когда сравниваемые ″хвосты″ последовательностей имеют одинаковое число $2^{n-2} - 2$ единиц и нулей. Мы пришли к противоречию, и, следовательно, предположение, что $s \neq t$ неверно.

Таким образом, среди $2k$ пар совпадений признаков ″чет″ и ″нечет″ в равенствах $\lambda(\alpha,\beta)$ для каждой подстановки половина совпадений ″четы″ и еще половина – ″нечеты″.

Перейдем теперь к определению значений интересующего нас числа $\lambda(\alpha,\beta)$ для подстановки порядка 2^n.

Заметим сразу, что подстановки с одним и тем же значением параметра $\lambda(\alpha,\beta)$ отличаются друг от друга распределением в левой и правой сторонах равенств $\alpha \cdot P = \beta \cdot C$ четных и нечетных компонент.

Ранее уже отмечалось, что из 2^n скалярных произведений в правых частях равенств (как и в левых) половина произведений имеют признак ″чет″, а другая половина признак ″нечет″ (их 2^{n-1} каждого типа). Причем равенство сохраняется, если меняются местами между собой переходы (выходы) подстановки, которые дают результатами скалярные произведения с одинаковым признаком четности.

Это значит, что для каждого значения маски выходов β существует $2^{n-1}!$ различных подстановок, отличающихся между собой закреплением (расстановкой) выходов, формирующих признаки ″чет″ и столько же, т.е. $2^{n-1}!$ различных подстановок, отличающихся между собой закреплением выходов, формирующих признаки ″нечет″.

В силу независимости распределения выходов подстановок по входам всего получается, что существует $(2^{n-1}!)^2$ вариантов различных подстановок, имеющих одно и то же распределение признаков ″чет″ и ″нечет″ (2^{n-1} скалярных произведений $\beta \cdot C$ каждого типа четности), отличающихся закрепленными за ними выходами подстановок.

Теперь каждая из таких подстановок реализует интересующее нас значение параметра $\lambda(\alpha,\beta) = 2k$ привязкой (совпадениями признаков ″чет″ и ″нечет″) $2k$ скалярных произведений $\beta \cdot C$ выходов к $2k$ скалярным произведениям входов $\alpha \cdot P$.

В соответствии с утверждением 2 таких совпадений будет в $2k$ переходах $\lambda(\alpha,\beta)$ по k каждого типа четности. Эти два набора по из одинакового числа переходов каждого типа (k равенств $\alpha \cdot P = \beta \cdot C$ каждого из типов) могут быть осуществлены для каждого уникального набора из 2^{n-1} скалярных произведений $\beta \cdot C$ одного типа четности $C^k_{2^{n-1}}$ вариантами расстановки выходов подстановки по ее входам, а всего получается, что равенства обоих типов четности, образующих $2k$ интересующих нас переходов $\lambda(\alpha,\beta)$, могут быть реализованы

$$\left(C_{2^{n-1}}^{k}\right)^2 \qquad (2)$$

различными способами ($C_{2^{n-1}}^{k} = \begin{pmatrix} 2^{n-1} \\ k \end{pmatrix}$ – биномиальный коэффициент).

В результате приходим к результату, который и утверждается в теореме.

В линейном криптоанализе интересуются входами (значениями) в линейную аппроксимационную таблицу подстановки порядка 2^n, которые являются отличием (смещением) действительного значения на число 2^{n-1}, что представляет собой корреляцию между линейными комбинациями входов и выходов.

Поэтому рассматриваются так называемые линеаризованные таблицы подстановок, которые в [20] обозначены $LAT_\pi^*(\alpha,\beta)$. Они определяются выражением

$$LAT_\pi^*(\alpha,\beta) = \left| LAT_\pi(\alpha,\beta) - 2^{n-1} \right|. \qquad (3)$$

В этом случае модуль в правой части записанного соотношения приводит к тому, что значение $LAT_\pi^*(\alpha,\beta) = 2k$, $k > 0$ может быть получено и при $k' = k + 2^{n-1}$, и при $k' = 2^{n-1} - k$ (значение $k' = k - 2^{n-1}$ может быть как положительным, так и отрицательным). Причем, возможны и нулевые значения $LAT_\pi^*(\alpha,\beta)$, когда $k' = 2^{n-1}$. С учетом отмеченного приходим к утверждению 3.

Утверждение 3. *Пусть* $\lambda^*(\alpha,\beta)$ *будет случайным значением линейной аппроксимационной таблицы* $LAT_\pi^*(\alpha,\beta)$ *для пары её входов б и в, когда подстановка р выбрана равновероятно из множества* 2^n *и* α,β *не нулевые. Тогда* $\lambda^*(\alpha,\beta)$ *принимает только четные значения и для* $|k| \le 2^{n-2}$

$$\Pr\left(\lambda^*(\alpha,\beta) = 2k\right) = \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \left(\begin{matrix} 2^{n-1} \\ 2^{n-2} + |k| \end{matrix} \right)^2. \qquad (4)$$

Утверждение следует непосредственно из теоремы 1 и приведенных выше соображений.

2. СРАВНЕНИЕ РАСЧЕТНЫХ И ЭКСПЕРИМЕНТАЛЬНЫХ РЕЗУЛЬТАТОВ

Наша цель определить границу для наибольшего значения входа в LAT_π^*.

Пусть теперь, как и в [20], $\lambda(\pi)$ – будет наибольшим входом LAT_π^* для отображения π, взятого над всеми невырожденными α и β:

$$\lambda(\pi) \overset{def}{=} \max_{\alpha,\beta \ne 0} LAT_\pi^*(\alpha,\beta).$$

Рассуждения автора цитируемой работы [20] по определению $\lambda(\pi)$ не все представляются достаточно аккуратными. Кроме того, автор допускает ошибки в записи некоторых принципиальных соотношений. Поэтому мы, не игнорируя его отдельных соображений и рассуждений, представим свой вариант вывода расчетного выражения для определения $\lambda(\pi)$.

Итак, пусть теперь $E[\lambda(\pi,2k)]$ обозначает ожидаемое число ячеек таблицы LAT_π^*, имеющих значение $2k$.

В этом месте, как и в работе [20], мы и сделаем переход от свойств ансамбля подстановок к свойствам отдельной подстановки, о чем говорилось в предыдущем разделе. Считая, что полученный закон распределения вероятностей (4) справедлив для каждой отдельно взятой подстановки, рассмотрим его теперь применительно к множеству $(2^n - 1)^2$ ячеек таблицы LAT_π^*, соответствующих ненулевым ее входам и выходам.

В результате мы можем получить выражение для вычисления $E[\lambda(\pi,2k)]$ как простое умножение формулы (4) на общее число ячеек таблицы подстановки, исключая первую строку и первый столбец

$$E[\lambda(\pi,2k)] = \frac{(2^n-1)^2 \cdot \left(2^{n-1}!\right)^2}{2^n!} \cdot \left(\begin{matrix} 2^{n-1} \\ 2^{n-2} + |k| \end{matrix} \right)^2, \qquad (5)$$

(для положительных и отрицательных значений смещения k результат будет один и тот же).

Аналогичный результат получен и в работе [21], однако, и в записи этого выражения, как и в записи выражения аналогичного выражению (4), в цитируемой работе имеются погрешности.

Выражение (5) имеет тенденцию быстро стремиться к нулю с ростом k. Среднему значению максимума таблицы LAT_π^* подстановки, как следует из сопоставления результатов вычислений с экспериментальными данными, будет соответствовать значение k^*, при котором получается наименьшее значение $E[\lambda(\pi,2k)]$, превышающее или равное единице, т.е. для определения k^* необходимо найти округленное в сторону увеличения до ближайшего целого решение уравнения

$$\frac{(2^n-1)^2 \cdot \left(2^{n-1}!\right)^2}{2^n!} \cdot \left(\begin{matrix} 2^{n-1} \\ 2^{n-2} + |k^*| \end{matrix} \right)^2 = 1. \qquad (6)$$

Аналогичный результат представлен в работе [20] в виде условия для определения границы для вероятности того, что $\lambda(\pi)$ достигает самое большее значение $2t$ в виде

$$\Pr(\lambda(\pi) \le 2t) > 1 - \sum_{k=2^{n-2}+t}^{2^{n-1}} E[\lambda(\pi,2k)].$$

В частности, автором определялось наименьшее значение t, для которого $\Pr(\lambda(\pi) \le 2t) > \frac{1}{2}$, и это граничное значение им было обозначено t_n и определено как медиана распределения. Результаты расчетов, приведенные в его работе, отличаются от полученных нами в два раза (из-за лишнего сомножителя двойки в представлении выражения (5)).

Варианты решения уравнения (6) (переборным методом, который резко упрощается при использовании результатов экспериментов), вместе с данными экспериментов иллюстрирует табл. 1.

Как следует из результатов, представленных в табл. 1, найденные значения максимумов таблиц

линейных аппроксимаций случайных подстановок хорошо согласуются с данными, полученными экспериментальным путем.

Таблица 1

Сравнение теоретических и экспериментальных результатов

n	$2k^*$	$E[\lambda(\pi,2k)]$	Эксперимент
4	4 6 8	3,89 1,118 0,017	5,498 $\left(\frac{3}{2}\right)^8 = 5{,}06$
6	12 14 16	9,013 1,7 0,239	14,48 $\left(\frac{3}{2}\right)^6 = 11{,}39$
8	32 34	2,12 0,7457	34,68 $\left(\frac{3}{2}\right)^8 = 25{,}62$
10	74 76	1,16 0,64	78,8 $\left(\frac{3}{2}\right)^8 = 57{,}66$
12	162 164	1,129 0,82	116,24 $\left(\frac{3}{2}\right)^8 = 129{,}74$
14	350 352	1,069 0,900	314 $\left(\frac{3}{2}\right)^{14} = 291$
16	748 750	1,027 0,93	720 $\left(\frac{3}{2}\right)^{17} = 657$

Если идти далее, то можно убедиться, что закон распределения вероятностей (4) с ограничением по числу слагаемых можно рассматривать как закон распределения вероятностей значений $\lambda^*(\alpha,\beta)$ таблицы $LAT_\pi^*(\alpha,\beta)$ отдельной взятой случайной подстановки π (к аналогичному результату в отношении закона распределения вероятностей значений ячеек XOR таблиц мы пришли и в работе [19] при анализе дифференциальных свойств случайных подстановок).

Убедимся, что для найденной нами вероятности (4) выполняется условие нормировки (проверка результата).

Запишем для этого более аккуратное выражение для вероятности того, что $\lambda(\pi)$ имеет значение не превышающее $2t$ в виде

$$\Pr\left(\lambda^*(\alpha,\beta)\le 2t\right)=\sum_{k=-t}^{t}\Pr\left(\lambda^*(\alpha,\beta)=2k\right)= \\ =\sum_{k=2^{n-2}-t}^{2^{n-2}+t}\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{k}^2, \qquad (7)$$

для $t\le 2^{n-2}$.

Если воспользоваться известным свойством биномиальных коэффициентов:

$$\left(C_n^0\right)^2+\left(C_n^1\right)^2+\ldots+\left(C_n^n\right)^2=C_{2n}^n$$

(см., например, [21]), то приходим к результату $\Pr\left(|\lambda(\pi)|\le 2^{n-1}\right)=1$, т.е. условие нормировки для закона распределения вероятностей (4) выполнено.

Более того, легко убедиться также в том, что

$$2\cdot\sum_{k=k^*+1}^{2^{n-2}}\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+k}^2<<1. \qquad (8)$$

Здесь мы рассматриваем только положительные значения смещения, а наличие и отрицательных значений учитывается введением множителя двойки. В таблице 2 представлены результаты расчетов суммы в левой части выражения (8), выполненные для различных сочетаний параметров n и k^*.

Таблица 2

Оценка "Хвостов" распределений

n	$2k^*$	$\sum_{k=k^*+1}^{2^{n-2}}\Pr\left(\lambda^*(\alpha,\beta)=2k\right)$	$\left(2^{n-1}-1\right)^2\sum_{k=k^*+1}^{2^{n-2}}\Pr\left(\lambda^*(\alpha,\beta)\right)$
4	8	0,00007	0,016
6	16	$1{,}66\cdot 10^{-6}$	0,0065
8	34	0,0000168	1,09
10	72	$4{,}4\cdot 10^{-6}$	4,6
12	156	$6{,}299\cdot 10^{-7}$	11,065
14	336	$8{,}24\cdot 10^{-8}$	8,69

И в этом случае, как и в предыдущей нашей работе [19], мы экспериментально установили, что отмеченные выше результаты характерны не только для случайных подстановок, но и для многоцикловых шифрующих преобразований, свойственных блочным симметричным шифрам во блочным симметричным шифрам вообще. Наши эксперименты показывают, что шифрующее преобразование (любой современный шифр) асимптотически (для Rijndael подобных шифров уже после 4-х циклов) для различных ключей зашифрования ведет себя как случайная подстановка, т.е. и для них оказываются справедливыми расчетные соотношения, представленные в этой работе, относящиеся теперь к линейным аппроксимациям. Для иллюстрации этого факта в табл. 3 представлены результаты определения значений числа "переходов" $\lambda^*(\alpha,\beta)$ таблицы $LAT_\pi^*(\alpha,\beta)$ линейного корпуса (таблицы LAT_π^* для 4-х циклового шифрующего 16-битного преобразования) уменьшенной модели шифра Лабиринт (одного из шифров, представленных на Украинский конкурс по выбору нового стандарта блочного симметричного преобразования). Аналогичные результаты получаются и для уменьшенных моделей других шифров: Baby Rijendael, Baby ADE и др.

Luka O'Connor и в работе [21] применяет свои результаты только к шифрам, использующим случайные подстановки, и как во многих известных работах, посвященных оценке стойкости БСШ к атакам линейного криптоанализа,

Таблица 3

Отклонение	0	2	100	200	300	400	500	600	720
Количество	81839	163317	120328	48060	10378	1232	82	1	1

показатели стойкости шифров он связывает с линейными свойствами подстановочных преобразований, использованных при их построении. Как мы уже отмечали в предыдущей нашей работе [19], полученные нами с использованием уменьшенных моделей шифров Rijndael, Камелия, а также шифров Мухомор, Лабиринт, Калина и ADE, представленных на Украинский конкурс по выбору национального стандарта блочного симметричного шифрования, а также ряда других шифров, экспериментальные результаты свидетельствуют о том, что реальные асимптотические (при полных наборах цикловых преобразований) значения максимальных и средних вероятностей дифференциальных и линейных характеристик (полных дифференциалов и линейных корпусов) для этих шифров являются свойством, не зависящим ни от свойств S-блоков, ни от числа циклов (после определенного их числа), ни от способа введения в цикловые функции подключей [22]. Они определяются, как уже было отмечено выше, свойствами шифрующего преобразования именно как случайной подстановки, несмотря даже на то, что БСШ реализует существенно меньшую часть всего множества подстановок соответствующего порядка.

ЗАКЛЮЧЕНИЕ

Перейдем теперь к выводам в отношении формирования оценок показателей стойкости БСШ к атакам линейного криптоанализа.

Представляется, что и в этом случае (как и в работе [19]) в качестве показателя эффективности, позволяющего сравнивать между собой различные решения по построению БСШ, можно использовать число циклов шифрования, после которого достигается асимптотическое значение максимума таблицы линейных аппроксимаций шифра.

Для определения этого асимптотического значения предлагается рассматривать наряду с приведенными выше расчетными соотношениями, воспользоваться которыми для больших шифров по-видимому не удастся, более простое соотношение, возникшее в процессе изучения результатов вычислительных экспериментов в виде

$$\lambda(\pi)=\left(\frac{3}{2}\right)^n.$$

Остается привести расчетное соотношение для определения максимума линейной вероятности.

Напомним, что в обозначениях работы [17] максимальная линейная вероятность $DL^f_{\max}$ для ключезависимой функции f с n-битным входом x и n-битным выходом y ($(x, y \in GF(2)^n)$ есть

$$DL^f_{\max} = \max_{Ax, AY \neq 0} DL^f(Ay \to Ax),$$

где

$$DL^f(\ y \to\ x) =$$

$$= \left(\frac{\#\{x \in GF(2)^n / x \cdot Ax = f(x) \cdot Ay\}}{2^{n-1}} - 1 \right)^2.$$

Связь записанных соотношений с приведенными в работе очевидна

$$DL^f_{\max} = \left(\frac{\lambda(\pi)}{2^{n-1}} \right)^2.$$

В заключение остается еще раз напомнить, что линейные свойства шифрующих преобразований современных блочных симметричных шифров (при заявленном числе циклов преобразования) являются одним из проявлений свойств случайных подстановок, и в этом смысле шифр Rijendael и шифры, представленные на Украинский конкурс, являются эквивалентными. Все они реализуют наибольшую вероятность максимума линейного корпуса (для 128 битных версий) близкую к значению

$$\left(\frac{\left(\frac{3}{2}\right)^{128}}{2^{127}} \right)^2 = 2^{-104}.$$

Литература.

[1] *C.M. Adams.* A formal and practical design procedure for Substitution-Permutation network cryptosystem. PhD thesis, Department of Electrical Engineering, Queen's University at Kingston, 1990.

[2] *C. M. Adams. And S.E. Tavares.* The Structured design of cryptographically good S-boxes. Journal of Cryptology, 3 (1): 27-41, 1990.

[3] *R. Forré.* Methods and instruments for designing S-boxes. Journal of Cryptology, 2(3): 115-130,1990.

[4] *K. Nyberg.* Perfect nonlinear S-boxes. In Advances in cryptology - EUROCRYPT91, volume 547, Lecture Notes in Computer Science, pp. 378-386. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[5] *E.F. Brickell, J.H. Moore, and M.R. Purtill.* Structure in the S-boxes DES. Advances in cryptology, CRYPTOZb, Lecture Notes in Computer Science, vol. 263.A.M. Odlyzko ed., Springer-Verlag, pages 3-8, 1987.

[6] *M.H. Dawson.* A unified framework for substitution box design based on information theory. Vaster's thesis, Queen's University, Kingston, Ontario, Canada, 1991.

[7] *E. Biham, A. Shamir.* Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, Vol. 4 No.l, 1991, pp. 3-72.

[8] *Matsui, M.:* Linear cryptanalysis method for DES cipher. In Advances in Cryptology.- EUROCRYPT'93 (1994) vol. 765. Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 386-397.

[9] *K. Nyberg and L.R. Knudsen*. Provable security against differential cryptanalysis. In Advances in cryptology - EUROCRYPT'92, volume Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, 1992, pp. 566-574.

[10] *T. Beth and C. Ding*. On permutations against differential cryptanalysis. In Advances in cryptology - EUROCRYPT'93. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[11] *K. Nyberg*. Differentially uniform mappings for cryptography. In Advances in cryptology - Proceedings of EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York, pp. 55-65.

[12] *Seberry J., Zhang X.M., Zheng Y.* "Pitfalls in Designing Boxes (Extended Abstract)"//, Copyright © Springer-Verlag, 1998, pp. 383-396.

[13] *Seberry J., Zhang X.M., Zheng Y.:* Relationships among nonlinearity criteria. Presented at EUROCRYPTV4, 1994.

[14] *Zhang X.M, Zheng Y, Imai. H.:* Non-existence of Certain Quadratic S-boxes and Two Bounds on Nonlinear Characteristics of General S-boxes // October 1997, pp. 1-18.

[15] *K. Nyberg*. On the construction of highly nonlinear permutations. In Advances in cryptology - Proceedings of EUROCRYPT'92 (1993) vol. 740, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 92-98.

[16] *Seberry J., Zhang X.M., Zheng Y.* Improving the strict avalanche characteristics of cryptographic functions. Information Processing Letttrs, 50:37-41, 1994.

[17] *F. Sano, K. Ohkuma, H. Chimisu, and S. Rawamura*. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis, IEISE Trans. Fundamentals, VOL. E86-A, No.1, pp. 37–46, Janiary 2003.

[18] *Алексийчук А.Н., Ковальчук Л.В., Скрыпник Е.В., Шевцов А.С.* Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах // Прикладная радиоэлектроника: научн.-техн. журнал. – 2008, Т. 7, № 3. – С. 203–209.

[19] *Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д.* Дифференциальные свойства случайных подстановок. // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010. – Т.9. – № 3. – С. 326–333.

[20] *Luke O'Connor*. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995.

[21] *Luke O'Connor*. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995. (семь страниц).

[21] *Бронщтейн И.Н., Семендяев К.А.* Справочник по математике для инженеров и учащихся вузов. – М.: "Наука", 1980. – 197 с.

[22] *Долгов В. И., Лисицкая И. В., Олешко О. И., Золочевская А. Ю., Дроботько Е. В.* К вопросу оценки стойкости БСШ к атакам линейного и дифференциального криптоанализа. Сборник трудов Первой Международной научно-технической конференции "Компьютерные науки и технологии", 8-10 октября 2009 г., Белгород, Ч. II. – С. 35-39.

Поступила в редколлегию 25.06.2010.

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Олешко Олег Иванович, старший преподаватель кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

УДК 621. 391:519.2:519.7

Властивості таблиць лінійних апроксимацій випадкових підстановок / В.І. Долгов, І.В. Лисицька, О.І. Олешко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 334-340.

Виводяться розрахункові співвідношення для середнього значення максимумів таблиць лінійних апроксімацій випадкових підстановок. Показується, що лінійні властивості шифруючих перетворень сучасних блокових симетричних шифрів (при заявленому числі циклів перетворення) є одним із проявів властивостей випадкових підстановок. Пропонується підхід до порівняння ефективності рішень з побудови алгоритмів шифрування у вигляді мінімального числа циклів алгоритму, при якому реалізується асимптотичний показник середнього значення максимуму лінійного корпусу.

Ключові слова: лінійні апроксимації, випадкові підстановки.

Табл. 03. Бібліогр.: 22 найм.

UDC 621. 391:519.2:519.7

Properties of tables of linear approximations of random substitutions / V.I. Dolgov, I.V. Lisitskaya, O.I. Oleshko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 334-340.

Computational relations for the average maximum value of tables of linear approximations of random substitutions are derived. It is shown that the linear properties of encryption transformations of modern block symmetric ciphers (with the declared number of transformation cycles) are one of the manifestations of properties of random substitutions. The paper suggests an approach to comparing the efficiency of solutions on construction of encryption algorithms in the form of a minimum number of cycles of an algorithm, which implements an asymptotic index of the average maximum value of a linear hull.

Key words: linear approximation, random substitutions.

Tab. 03. Ref.: 22 items.

УДК 681.3.06

ОЦЕНКА ЧИСЛА СЛУЧАЙНЫХ ПОДСТАНОВОК С ЗАДАННЫМ РАСПРЕДЕЛЕНИЕМ ПЕРЕХОДОВ XOR ТАБЛИЦ И СМЕЩЕНИЙ ТАБЛИЦ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ

И.В. ЛИСИЦКАЯ, А.В. ШИРОКОВ, Е.Д. МЕЛЬНИЧУК, К.Е. ЛИСИЦКИЙ

Определяются значения показателей отбора (% прохождения) подстановок, обладающих теоретическими значениями законов распределения переходов из XOR таблиц и смещений таблиц линейных аппроксимаций. Приводятся результаты экспериментальной проверки теоретически обоснованных значений показателей отбора.

Ключевые слова: случайная подстановка, таблица XOR разностей подстановки, таблица линейных аппроксимаций подстановки, критерии отбора случайных подстановок, закон распределения переходов таблиц XOR разностей случайной подстановки, закон распределения смещений таблицы линейных аппроксимаций случайной подстановки.

ВВЕДЕНИЕ

В этой работе мы продолжим обсуждение введенных в наших предыдущих работах [1,2] двух новых (дополнительных) критерия отбора случайных подстановок. Здесь обосновываются окончательные (предлагаемые для практического использования) граничные значения параметров b и c в критериях отбора (по Колмогорову) и приводятся примеры практического применения этих критериев для отбора подстановок с ожидаемыми улучшенными криптографическими показателями.

1. ЗАКОНЫ РАСПРЕДЕЛЕНИЯ ПЕРЕХОДОВ ТАБЛИЦ XOR РАЗНОСТЕЙ СЛУЧАЙНЫХ ПОДСТАНОВОК И СМЕЩЕНИЙ ТАБЛИЦЫ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ ПОДСТАНОВКИ

Нас будут интересовать сначала подстановки, таблицы XOR разностей которых имеют заданное распределение парных разностей (переходов входных разностей ΔX в соответствующие выходные разности ΔY).

В обозначениях работы [3] пусть $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$ будет вероятностью того, что значение ячейки дифференциальной таблицы случайно взятой подстановки π порядка 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно $2k$. Эта вероятность определяется теоремой [3].

Утверждение 1. *Для любых ненулевых фиксированных* $\Delta X, \Delta Y \in Z_2^n$ *в предположении, что подстановка* π *выбрана равновероятно из множества подстановок симметрической группы и* $0 \le k \le 2^{n-1}$,

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right) = \left(\begin{array}{c}2^{n-1}\\ k\end{array}\right)^2 \cdot \frac{k!\cdot 2^k \cdot \Phi(2^{n-1}-k)}{2^n!}, \quad (1)$$

где функция $\Phi(d)$ определяется выражением

$$\Phi(d)=\sum_{i=0}^{d}(-1)^i \cdot \left(\begin{array}{c}d\\ i\end{array}\right)^2 \cdot 2^i \cdot i! \cdot (2d-2i)!. \quad (2)$$

В [3] также получено соотношение для среднего значения числа ненулевых характеристик отдельного S-блока с переходами $\Delta X \to \Delta Y$, такими, что $\Lambda_\pi(\Delta X,\Delta Y)=2k$:

$$\Lambda_{m,2k}=\frac{(2^m-1)^2}{2^m!}\cdot\left(\begin{array}{c}2^{m-1}\\ k\end{array}\right)^2 \cdot k!\cdot 2^k \cdot \Phi(2^{m-1}-k). \quad (3)$$

Предыдущим обозначениям в (3) соответствует $m=n$.

Для иллюстрации в табл. 1 представлены результаты расчетов, выполненных по этому выражению, для подстановки 16-той степени ($m=4$).

Таблица 1

Распределение парных разностей для XOR таблицы подстановки порядка 2^4 (расчёт)

$2k$	Число ячеек	Вероятность
0	132,165	0,587399
2	70, 1592	0,311819
4	18,7723	0,0834326
6	3,381	0,0150289
8	0,4662	0,002072

В табл. 2 представлены результаты расчетов для подстановок порядка 2^8 [2].

Аналогичные соотношения в работах [1, 2] были рассмотрены для законов распределения переходов таблиц линейных аппроксимаций – ЛАТ (законов распределения вероятностей линейных корпусов).

Таблица 2

Распределение парных разностей для XOR таблицы подстановки порядка 2^8 (расчёты с округлением в сторону ближайшего целого)

$2k$	Число ячеек	Вероятность
0	39363	0,605345
2	19758	0,303855
4	4959	0,0762627
6	830	0,0127609
8	104	0,001599
10	10	0,00015378
12	1	0,000015378

В работе [1] было предложено использовать вычисленные таким образом законы распределения парных разностей и смещений ЛАТ подстановок различного порядка для построения новых (дополнительных) критериев отбора случайных подстановок. В последующей работе [2] были рассмотрены вопросы установления границ при использовании критерия Колмогорова для оценки близости законов распределения переходов дифференциальных и линейных таблиц подстановок теоретическим (мы их назвали ″эталонными″), на основе результатов которых принимается решение можно ли отнести проверяемую подстановку к случайной или нет. В этой работе нас будут интересовать вопросы практической реализуемости подстановок с ″предельными″ показателями, т.е. показателями, соответствующими ″эталонным″.

Отметим здесь, что новые критерии построены на идее подчинения свойств подстановок свойствам шифрующих преобразований. Заметим также, что для шифрующих преобразований, рассматриваемых как подстановки, законы распределения переходов дифференциальных и линейных таблиц, если переходить на терминологию работы [4], представляют собой законы распределения полных дифференциалов и линейных корпусов.

2. ТЕОРЕТИЧЕСКАЯ ОЦЕНКА ОЖИДАЕМОГО ЧИСЛА ПОДСТАНОВОК С ЗАДАННЫМИ ЗАКОНАМИ РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ ПЕРЕХОДОВ ДИФФЕРЕНЦИАЛЬНЫХ И ЛИНЕЙНЫХ ТАБЛИЦ

Будем интересоваться теоретически ожидаемым числом подстановок из общего их множества $2^n!$, которые соответствуют ″эталонному″ закону распределения вероятностей. Эти результаты одновременно станут теоретическим обоснованием экспериментальных результатов, приведенных в работе [2].

Здесь определяющим для последующих шагов может стать достаточно очевидное соображение, заключающееся в том, что подстановками с требуемыми свойствами будут те, которые имеют непременно переход с максимальным значением полного дифференциала k_D^* (присутствующим в эталонном распределении).

Но k_D^* – это значение, при котором выражение (3) (см. [3]) принимает значение близкое к единице (Для ЛАТ k_L^* – это значение, при котором уравнение аналогичное (3) (см. [4]) принимает значение близкое к единице).

В соответствии с логикой получения выражения (1) его числитель определяет число подстановок, имеющих значение ячейки XOR таблицы для перехода ΔX в ΔY равное $2k$. Следовательно, вычислив значение этого соотношения при $k = k_D^*$, мы можем найти теоретическое значение вероятности получения (формирования) при случайном выборе подстановки, имеющей переход XOR таблицы равный $2k_D^*$, т. е. вероятность, обозначенную в предыдущей нашей работе [3] $Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right)$.

Этот переход (единственный в подстановке переход с максимальным значением) может присутствовать (появиться) на любой позиции (в любой ячейке) подстановки (в любой строке таблицы).

Учитывая, что каждая подстановка имеет $2^n - 1$ ненулевых строк (столбцов), приходим к выводу, что вероятность получить отдельную подстановку с необходимым для нас переходом (с максимальным значением) на любой из $2^n - 1$ возможных позиций (строк или столбцов) равна сумме вероятностей $2^n - 1$ независимых равновероятных событий, т. е.

$$Pr\Big(\Lambda_\pi(\Delta X_1,\Delta Y_1) = 2k_D^*, \Lambda_\pi(\Delta X_2,\Delta Y_2) = 2k_D^*,$$
$$\ldots, \Lambda_\pi(\Delta X_{2^{n-1}},\Delta Y_{2^{n-1}}) = 2k_D^*\Big) =$$
$$= (2^n - 1)\cdot Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right).$$

Это и есть тот результат, который нам нужен и с помощью которого мы можем получить интересующие нас оценки для вероятностей получения подстановок с дифференциальными и линейными таблицами, повторяющими расчетные распределения таблицы 1 и соответствующих таблиц для переходов линейных таблиц аппроксимаций случайных подстановок.

Остается заметить, что если учесть также то, что умножение вероятности $Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right)$ еще раз на число $2^n - 1$ приводит в соответствии с соображениями [3] к результату:

$$(2^n - 1)^2 \cdot Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right) \approx 1,$$

т.е. мы имеем дело с полной группой событий, что отражает тот очевидный факт, что каждая таблица имеет хотя бы одну ячейку со значением k_D^* (сумма вероятностей $Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right)$ для всех ячеек подматрицы A_π таблицы XOR разностей).

В результате для определения вероятности интересующего нас события – выбора подстановки с заданным законом распределения вероятностей переходов) можно получить оценочное выражение в виде:

$$Pr\Big(\Lambda_\pi(\Delta X_0,\Delta Y_0) = 0, \Lambda_\pi(\Delta X_1,\Delta Y_1) = 2,$$
$$\Lambda_\pi(\Delta X_2,\Delta Y_2) = 4, \ldots, \Lambda_\pi(\Delta X_s,\Delta Y_s) = 2k_D^*\Big) \le \frac{1}{2^n - 1},$$

и при этом

$$\#(\Delta X_0,\Delta Y_0) + \#(\Delta X_1,\Delta Y_1) + \#(\Delta X_2,\Delta Y_2) + \ldots +$$
$$+ \#(\Delta X_s,\Delta Y_s) = (2^n - 1)^2,\ s = k_D^*,$$

которое и предлагается использовать для дальнейших расчетов.

Очевидно, что совершенно аналогичное выражение может быть получено и для оценки вероятности случайного выбора подстановки с таблицей линейных аппроксимаций, повторяющей "эталонную":

$$Pr\left(\Lambda_\pi(\alpha_0,\beta_0)=0,\Lambda_\pi(\alpha_1,\beta_1)=2,\right.$$

$$\left.\Lambda_\pi(\alpha_2,\beta_2)=4,\ldots,\Lambda_\pi(\alpha_s,\beta_s)=2k_L^*\right)\le\frac{1}{2^n-1}.$$

Здесь уже

$$\#(\alpha_0,\beta_0)+\#(\alpha_1,\beta_1)+\#(\alpha_2,\beta_2)+\ldots+$$

$$+\#(\alpha_s,\beta_s)=(2^n-1)^2,\ s=k_L^*.$$

В итоге для практически интересных ситуаций использования в шифрах S-блоков размерами битовых входов равными $n=4$ и $n=8$ для вероятностей получения (генерации) S-блоков случайного типа с параметрами таблиц XOR разностей и линейных аппроксимаций, повторяющих теоретические распределения таблиц 1-4, приходим к значениям:

$$n=4\ \rightarrow\ 2^4-1=15\ \rightarrow$$

$$\rightarrow\ Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=8)\right)=\frac{1}{15}=0{,}06(6);$$

$$n=8\ \rightarrow\ 2^8-1=255\ \rightarrow$$

$$\rightarrow\ Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=12)\right)=\frac{1}{155}=0{,}004.$$

Совершенно аналогичные результаты получаются и для подстановок с соответствующими таблицами линейных аппроксимаций.

Считая теперь, что дифференциальные и линейные показатели подстановок независимы, для вероятности получить при случайном выборе подстановку, обладающую одновременно максимальными значениями ячеек таблиц XOR разностей и линейных аппроксимаций равными k_D^* и k_L^*, приходим к результату (в худшем случае):

$$n=4\ \rightarrow\ 2^4-1=15\ \rightarrow$$

$$\rightarrow Pr\left(\Lambda_\pi\{(\Delta X,\Delta Y)=k_D^*),(\alpha,\beta\right)=k_L^*\}=$$

$$=(0{,}06(6))^2\approx 0{,}004.$$

$$n=8\ \rightarrow\ 2^8-1=255\ \rightarrow$$

$$\rightarrow Pr\left(\Lambda_\pi\{(\Delta X,\Delta Y)=k_D^*),(\alpha,\beta\right)=k_L^*\}=$$

$$=(0{,}004)^2\approx 0{,}000016.$$

В соответствии с этими результатами (полученными теоретическим путем) выходит, что из общего числа 16! подстановок порядка $2^4=16$

– около 7% подстановок имеют дифференциальные или линейные свойства, повторяющие теоретические распределения, свойственные случайным подстановкам, из них ожидается, что одновременно имеют интересующие нас дифференциальные и линейные показатели примерно 0,4% всех подстановок.

Для подстановок порядка $2^8=256$ соответствующие показатели прохода (удовлетворения) критериев случайности имеют значения:

0,04% при раздельной фильтрации по дифференциальным или линейным показателям и

0,0016% при одновременном удовлетворении дифференциальных и линейных показателей отбора.

Приведенные цифры свидетельствуют, что реализация соответствующих параметров отбора для подстановок рассмотренного порядка вполне осуществима.

В итоге для отбора подстановок, удовлетворяющих новым критериям случайности, теоретически можно использовать самые жесткие ограничения (нулевые значения параметров b и c).

Результаты экспериментов с отбором случайных подстановок в целом подтвердили теоретически полученные значения вероятностей и по дифференциальным и по линейным показателям.

Эксперименты, однако, также показали, что подстановок, удовлетворяющих одновременно двум показателям случайности (одновременно и дифференциальным и линейным показателям) найти не удалось. Поэтому в процессе экспериментов были определены возможности минимального изменения границ отбора, при которых удалось достигнуть одновременного выполнения двух предлагаемых критериев. Опять-таки экспериментальным путем установлено, что достаточно, оказалось, ввести допустимые расхождения между эталонными и реальными значениями ворот отклонений от эталонных целочисленных значений в пределах ±2 единиц. В итоге, в пересчете на значения параметров b и c мы пришли к граничным значениям параметров отбора случайных подстановок.

Для подстановок порядка $2^4=16$:

$$b=c=\frac{2}{15^2}=0{,}008(8).$$

Для подстановок порядка $2^8=256$:

$$b=c=\frac{2}{255^2}=0{,}00003.$$

Примеры подстановок, отобранных с помощью представленных уточненных критериев, представлены в таблицах 3-4.

Таблица 3

Подстановки порядка 2^4 прошедшие отбор с параметрами критериев случайности $a=1$, $b=c=0{,}00889$

	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
S_1	2 8 14 5 7 9 1 13 12 11 15 4 6 0 10 3
S_2	0 6 9 5 15 13 8 7 4 3 14 1 11 12 10 2
S_3	9 5 11 4 6 14 10 8 2 15 12 13 0 1 7 3
S_4	2 8 14 5 7 9 1 13 12 11 15 4 6 0 10 3
S_5	10 15 12 1 8 2 14 0 9 11 3 13 6 4 7 5
S_6	9 5 11 4 6 14 10 8 2 15 12 13 0 1 7 3

В этом эксперименте из 1000 сгенерированных подстановок удовлетворили установленным критериям 8-мь подстановок (0,8%).

1000 подстановок такого порядка на компьютере с процессором AMD Sempron 2500+BOX требует порядка 30 минут времени. Это значит, что для проверки выборки объемом 1000000 потребуется 30 000 минут, что приводит к общему времени анализа ≈ 20 дней. Поэтому мы здесь приведем пример формирования (отбора) подстановки порядка 2^8 не с предельными показателями.

На рис. 1 представлен пример такой подстановки вместе с ее характеристиками.

Таблица 4

Пример подстановки порядка 2^8, прошедшей критерии отбора: $a > 1$, $b = 0{,}0002153$, $c = 0{,}00035417$

67	7e	4c	86	6	66	2d	dd	ee	c1	21	6b	bd	7d	26	fd
9d	7c	C9	2	3	f4	79	e	a0	2c	a9	8f	c5	74	b7	3d
68	72	af	3b	43	1a	63	3a	88	fb	C4	70	7b	5a	76	B8
5c	1e	39	41	8e	96	e9	b1	5	42	e7	de	c3	a4	17	7f
b	e5	0	4d	d2	ec	bc	87	18	94	85	a	34	d	9b	46
bb	f3	2f	aa	3e	7a	ba	dc	91	3c	37	4	33	93	83	e4
e6	4f	64	9f	5d	29	ea	78	65	c2	28	f9	12	e1	47	fa
b2	ac	25	d0	71	77	44	9e	2e	24	cb	a1	b6	c0	52	97
14	a7	22	ef	ad	ff	e3	90	10	bf	48	84	51	ca	d4	ae
F8	3f	56	92	5f	b4	6c	6a	c	d7	60	32	62	53	ce	b3
6d	a3	eb	6e	cc	50	54	b5	cf	9c	cd	c7	2a	c8	38	69
78	15	9a	80	59	d5	1f	5b	23	c6	ed	db	99	b0	1b	d1
F6	8d	f	b1	e0	4b	f1	a2	f0	98	d8	d3	f5	a5	27	35
73	fc	da	31	a6	36	2b	8c	57	61	1d	7	5e	81	11	9
6f	1	d9	a8	ab	8a	8b	fe	1c	f2	82	be	e8	45	4a	55
49	89	20	b9	df	e2	8	58	19	30	16	40	13	f7	95	d6

Cycles: 9
Inversions: 15321
Increasings: 131

Max DT: 12
Number of max DT: 1
MaxLAT: 34
Number of max LAT: 1

Elements DT:

0	39363
2	19758
4	4959
6	830
8	102
10	11
12	1
14	0
16	0
18	0
20	0
22	0
24	0
26	0
28	0
30	0
32	0
34	0

Max diversion: 0,0002153 (±14)

Elements LAT:

0	6465
2	12536
4	11404
6	9817
8	7839
10	5967
12	4255
14	2816
16	1778
18	1003
20	581
22	306
24	153
26	57
28	31
30	8
32	6
34	1

Max diversion: 0,00035417 (±23)

ЗАКЛЮЧЕНИЕ

Таким образом, мы показали, что существует достаточно большое число подстановок, имеющих законы распределения вероятностей переходов XOR разностей и смещений таблиц линейных аппроксимаций, повторяющие соответствующие законы распределения вероятностей случайных подстановок, полученные теоретическим путем.

Для подстановок порядка $2^4 = 16$ около 7% всех подстановок симметрической группы имеют дифференциальные или линейные свойства, повторяющие теоретические распределения, свойственные случайным подстановкам, из них ожидается, что одновременно имеют интересующие нас дифференциальные и линейные показатели

примерно 0,4% всех подстановок (отдельный эксперимент дал значение 0,8%).

Выполнение критериев случайности для инверсий, возрастаний и циклов приводит к дополнительному уменьшению допустимого множества на 50%.

Для подстановок порядка $2^8 = 256$ соответствующие показатели прохода (удовлетворения) критериев случайности имеют значение 0,0016% при одновременном удовлетворении дифференциальных и линейных показателей отбора.

Приведенные цифры свидетельствуют, что реализация соответствующих параметров отбора для подстановок рассмотренного порядка вполне осуществима.

И еще!

Можно сделать также вывод о том, что работоспособными оказываются намного более жесткие критерии отбора случайных подстановок, которые могут оказаться полезными при поиске подстановок с высокими криптографическими показателями.

По крайней мере, в разрешенное множество вошли подстановки, которые по своим свойствам повторяют свойства шифрующих преобразований.

Представляется, что с помощью таких подстановок удастся реализовать предельные показатели по скорости перехода шифрующих преобразований к асимптотическому режиму, определяемому с точки (момента), когда шифрующее преобразование приобретает свойства случайной подстановки. Найти убедительные аргументы в пользу плодотворности предлагаемого подхода станет задачей наших дальнейших исследований.

Литература

[1] *Лисицкая И.В., Лисицкий К.Е. Широков А.В., Мельничук Е.Д.* Случайные подстановки в криптографии // Радіоелектронні та комп'ютерні системи, 2010, № 5 (46), С. 79-84.

[2] *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 1997. Вып 103. – С. 121–130.

[3] *Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д.* Дифференциальные свойства подстановок // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010. Т. 9, № 3. – С. 326-333.

[4] *Долгов В.И., Лисицкая И.В., Олешко О.И.* Свойства таблиц линейных аппроксимаций случайных подстановок // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010. Т. 9, № 3. – С. 334-340.

Поступила в редколлегию 29.06.2010.

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Широков Алексей Викторович, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: криптоанализ.

Мельничук Евгений Дмитриевич, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: криптографическая защита информации.

Лисицкий Константин Евгеньевич, студент 1-го курса кафедры БИТ ХНУРЭ. Область научных интересов: криптографическая защита информации.

УДК 681.3.06

Оцінка числа випадкових підстановок із заданим розподілом переходів XOR таблиць і зміщенням таблиць лінійних апроксимацій / І.В. Лисицька, О.В. Широков, Є.Д. Мельничук, К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 341-345.

Визначаються значення показників відбору (% проходження) підстановок, що володіють теоретичними значеннями законів розподілу переходів їх XOR таблиць і зсувів таблиць лінійних апроксимацій. Наводяться результати експериментальної перевірки теоретично обгрунтованих значень показників відбору.

Ключові слова: випадкова підстановка, таблиця XOR різниць підстановки, таблиця лінійних апроксимацій підстановки, критерії відбору випадкових підстановок, закон розподілу переходів таблиць XOR різниць випадкової підстановки, закон розподіленості зміщень таблиці лінійних апроксимацій випадкової підстановки.

Табл. 04. Бібліогр.: 04 найм.

UDC 681.3.06

Estimating the number of random substitutions with a given distribution of transitions of XOR tables and shifts of tables of linear approximations / I.V. Lisitskaya, A.V. Shirokov, E.D. Melnichuk, K.E. Lisitskiy // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 341-345.

Values of indices of selecting (% of passing) substitutions having theoretical values of distribution laws of transitions of their XOR tables and shifts of tables of linear approximations are determined. The results of experimental verification of theoretically substantiated values of the indices of selection are given.

Key words: random substitution, XOR substitution difference table, linear approximations of substitution table, criteria for selection of random substitutions, law of distributing transitions of random substitution XOR difference tables, law of distributing shifts of the random substitution linear approximations table.

Tab. 04. Ref.: 04 items.

УДК 621. 391:519.2:519.7

КОМБИНАТОРНЫЕ СВОЙСТВА УМЕНЬШЕННОЙ ВЕРСИИ ШИФРА «КАЛИНА»

В.И. РУЖЕНЦЕВ, С.В. ЧИЧМАРЬ, Д.И. САВИН

Приводятся результаты исследования комбинаторных свойств мини версии шифра «Калина», одного из претендентов на национальный стандарт блочного симметричного шифрования Украины. Подтверждается, что законы распределения циклов, возрастаний и инверсий мини-шифра, рассматриваемого как подстановочное преобразование, повторяют свойства законов распределения вероятностей, характерные случайным подстановкам.

Ключевые слова: криптоанализ, шифр «Калина».

ВВЕДЕНИЕ

При выборе алгоритма шифрования нужно быть уверенным в том, что он будет обеспечивать необходимую стойкость защиты информации, а также будет иметь высокую скорость преобразований. Но всесторонний анализ криптографических алгоритмов требует больших вычислительных мощностей, а некоторые его аспекты вообще неосуществимы на данный момент. Для преодоления трудностей криптоанализа больших шифров на кафедре БИТ развивается подход, ориентированный на использование результатов анализа уменьшенных версий прототипов, для которых уже удается построить вычислительные эксперименты.

Важность развития работ в этом направлении определяется тем, что сейчас в Украине проходит конкурс по отбору претендентов на национальный стандарт блочного симметричного шифрования Украины и необходимы подходы, позволяющие ускорить процесс экспертизы представленных решений. Одних из предложений, рассматриваемых на этом конкурсе, является шифр «Калина».

Сегодня уже имеются результаты исследования циклических свойств шифрующих преобразований ряда мини версий шифров, представленных на Украинский конкурс [1]. Настоящая работа посвящена дальнейшему совершенствованию методики исследования комбинаторных свойств уменьшенных моделей шифров. В этой работе предлагаются построенные в ходе статистического эксперимента законы распределения инверсий, возрастаний и циклов уменьшенной модели шифра «Калина». Показывается, что полученные законы являются близкими к асимптотическим законам распределения, свойственным случайным подстановкам.

1. МЕТОДИКА ПОСТРОЕНИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ ЧИСЛА ИНВЕРСИЙ

В этом случае для каждого ключа зашифрования из полного множества всех ключей путем последовательных зашифрований (на одном и том же ключе) создаётся массив всех возможных вариантов зашифрованных блоков данных, начиная с зашифрования нулевого значения блока данных, и так последовательно до последнего значения входного блока данных (равного 2^{16}–1). Тем самым в массиве данных запоминается вторая строка нормализованного представления подстановки (шифрующего преобразования). Затем на основе последовательного просмотра и сравнения значений элементов массива с текущим, выбранным для анализа, выполняется подсчет числа инверсий, соответствующего рассматриваемому элементу массива (числа превышений значения текущего рассматриваемого элемента множества значений просмотренных элементов, стоящих в массиве правее рассматриваемого). Результат подсчета числа инверсий для каждого из последовательно выбранных элементов массива нижней строки подстановки отсылается в накапливающий счетчик, фиксирующий общее число инверсий, соответствующее текущей подстановке. Естественно, что потребуется использовать 2^{16} накапливающих счетчиков, чтобы затем построить, по данным счетчиков, закон распределения вероятностей для числа инверсий.

2. МЕТОДИКА ПОСТРОЕНИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ ЧИСЛА ЦИКЛОВ

В этом случае для каждого ключа зашифрования из полного множества ключей производится подсчет числа циклов подстановки, соответствующей каждому ключу. Поиск циклов и подсчет их числа производиться следующим образом. Создаётся массив всех возможных вариантов зашифрованных текстов, подобно тому, как это было сделано при анализе числа инверсий. Затем, начиная с нулевого значения элемента верхней строки подстановки (нулевого для зашифрования значения входного блока данных), выполняется зашифрование с последующим выполнением функции зашифрования к блокам данных, получающихся в результате зашифрования на текущем шаге. Значения результатов зашифрования фиксируются в исходном (запомненном) массиве путем исключения из него (или маркирования) появившихся в результате зашифрований значений. Эта операция выполняется до тех пор, пока в результате зашифрования не появится блок данных с нулевым значением (начальный блок

данных серии последовательных зашифрований). После этого выбирается наименьший по значению из оставшихся элементов массива (не попавший в предыдущий цикл), и строится новый цикл, начинающийся от нового значения, с запоминанием (″вычеркиванием″ или маркированием) пройденных (состоявшихся) зашифрованных значений. И эта процедура повторяется до тех пор, пока не будут пройдены (″вычеркнуты″) все элементы исходного массива. Параллельно с поиском циклов выполняется подсчет их числа с помощью соответствующего накапливающего счетчика. Для последующего построения закона распределения вероятностей для числа циклов используются дополнительный набор счетчиков, в которых подсчитывается число счетчиков, имеющих одинаковое заполнение, т.е. фиксирующих число подстановок (ключей зашифрования) с одним и тем же числом циклов.

3. МЕТОДИКА ПОСТРОЕНИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ ЧИСЛА ВОЗРАСТАНИЙ

И в этом случае создаётся массив всех возможных вариантов зашифрованных текстов (строится вторая строка нормализованного представления подстановки). Для подсчета числа возрастаний для каждого элемента массива производится подсчет числа элементов массива, имеющих следующий элемент массива больший по значению текущего. Число превышений (возрастаний), полученных для каждой подстановки, фиксируется соответствующим накапливающим счетчиком.

4. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ КОМБИНАТОРНЫХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «КАЛИНА»

Результаты исследования комбинаторных свойств, выполненные в соответствии с изложенными выше методиками, иллюстрируют таблица 1 и графические зависимости, представленные на рис. 1 и рис. 2. В табл.1 приведен закон распределении числа циклов шифра мини-Калина.

На рис. 1 и рис. 2 приведены графические зависимости, отражающие законы распределения вероятностей для числа инверсий и числа возрастаний шифра мини-Калина.

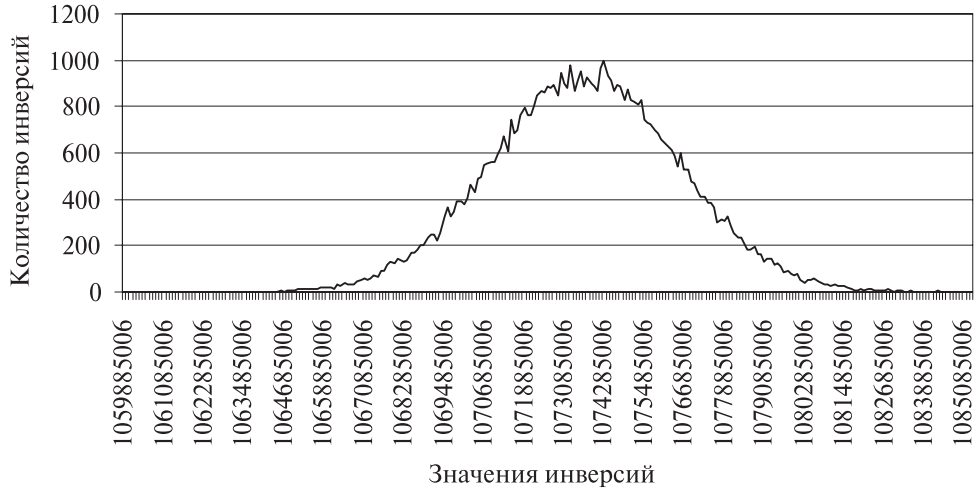


Рис. 1. Закон распределения числа инверсий для шифра мини-Калина

Рис. 2. Закон распределения числа возрастаний для шифра мини-Калина

Таблица 1

Закон распределения числа циклов шифра мини-Калина

Циклы	Количество
2	27
4	507
6	3234
8	9482
10	15318
12	16054
14	11524
16	6052
18	2407
20	706
22	186
24	34
26	5
28	1

ЗАКЛЮЧЕНИЕ

Представленные результаты свидетельствуют, что законы распределения числа циклов, возрастаний и инверсий шифра мини-Калина являются весьма близкими к нормальным, т.е. повторяют свойства, характерные для случайных подстановок [2]. Для определения числовых значений этих распределений можно пользоваться формулами для асимптотических законов распределения случайных подстановок.

Литература.

[1] *Долгов В.И., Олейников Р.В., Большаков А.Ю., Григорьев Ф.В., Дробатько Е.В.* Криптографические свойства уменьшенной версии шифра "Калина" // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010, Т. 9, № 3. – С. 349-354.

[2] *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. – Т. 6, № 2 – С. 257-263.

Поступила в редколлегию 2.07.2010.

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ, ХНУРЭ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров.

Чичмарь Сергей Владимирович, сотрудник кафедры БИТ ХНУРЕ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров.

Савин Дмитрий Игоревич, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: криптография, системы защиты информации.

УДК 621. 391:519.2:519.7

Комбінаторні властивості зменшеної версії шифру «Калина» / В.І. Руженцев, С.В. Чичмар, Д.І. Савін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 346-348.

Наводяться результати дослідження комбінаторних властивостей міні версії шифру «Калина», одного з претендентів на національний стандарт блокового симетричного шифрування України. Підтверджується, що закони розподілу циклів, зростання та інверсій мінішифру, що розглядається як підстановлювальне перетворення, повторюють властивості законів розподілу ймовірностей, характерні випадковим підстановкам.

Ключові слова: криптоаналіз, шифр «Калина».

Табл. 01. Іл.02. Бібліогр.: 2 найм.

UDC 621. 391:519.2:519.7

Combinatorial properties of reduced cipher «Kalina» / V.I. Ruzhentsev, S.V. Chichmar', D.I. Savin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 346-348.

The paper presents results of researching combinatorial properties of mini versions of the cipher «Kalina», one of the pretenders to the national standard of block symmetric encryption of Ukraine. It is confirmed that the laws of distributing cycles, increases and inversions of a mini-cipher, considered as a substitution transformation, follow properties of the laws of distributing probabilities which are characteristic of random substitutions.

Key words: cryptanalysis, cipher «Kalina».

Tab. 01. Fig. 02. Ref.: 02 items.

УДК 681.3.06

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА УМЕНЬШЕННОЙ ВЕРСИИ ШИФРА «КАЛИНА»

В.И. ДОЛГОВ, Р.В. ОЛЕЙНИКОВ, А.Ю. БОЛЬШАКОВ, А.В. ГРИГОРЬЕВ, Е.В. ДРОБАТЬКО

В первой части роботы приводится описание уменьшенной 16-битной версии шифра ″Калина″, а во второй – результаты исследования ряда криптографических показателей уменьшенной модели (циклические, дифференциальные, линейные и др. свойства).

Ключевые слова: симметричный блочный шифр, случайная перестановка.

ВВЕДЕНИЕ

В настоящее время в Украине проходит открытый конкурс по выдвижению и отбору кандидатов на национальный стандарт блочного симметричного шифрования. Одним из алгоритмов, представленных на данный конкурс, является алгоритм блочного симметричного шифрования ″Калина″.

На текущем этапе конкурса проходит изучение предложений экспертами и специалистами, а также ведется работа по проверке заявленных показателей стойкости и производительности.

Всесторонний анализ криптографических алгоритмов требует больших вычислительных мощностей, а некоторые его аспекты вообще неосуществимы на данный момент.

В широком спектре стоящих задач большое значение приобретает развитие и применение технологий, позволяющих ускорить процессы исследования и принятия решений. Одним из таких путей, направленных на создание и отработку эффективных методов сопоставления различных предложений, может стать, на наш взгляд, анализ криптографических показателей уменьшенных версий (моделей) шифров, в которых сохранены все принципиальные преобразования основного (большого) шифра. Естественно, здесь сразу возникает вопрос об адекватности перехода к версиям малых шифров (в смысле сохранения в модели всех свойств прототипа). Однако здесь можно положиться на достаточно очевидный принцип (назовем его постулатом): если хороши свойства модели, то свойства прототипа как минимум будут не хуже. Когда прототип поддается масштабируемости, то есть удается в модели сохранить структуру преобразований блоков данных и свойства основных операций, то результаты анализа свойств модели при определенных условиях, могут быть перенесены на прототип.

В этой работе предлагается уменьшенная модель шифра ″Калина″ [1] и изучаются ее ряд криптографических показателей.

При изложении материала мы в значительной степени будем опираться на описание шифров mini-AES [2] и большого шифра ″Калина″ [1].

1. ОПИСАНИЕ ШИФРА МИНИ-КАЛИНА

Алгоритм шифрования мини-Калина повторяет принципиальные решения, использованные при построении основной версии предложения [1], и практически является результатом масштабирования оригинальной разработки к размеру входного блока и ключа равному 16 битам. Как и в большом шифре, каждый 16-битный блок входных данных обрабатывается независимо от остальных. В процессе расшифрования используется тот же ключ, что и при шифровании. Шифртекст составляется из шифрованных блоков, последовательность которых соответствует очередности блоков открытого текста.

Нами были рассмотрены варианты построения алгоритма с десятью (как в оригинальной версии алгоритма) и с четырьмя циклами (для сравнения результатов с другими известными шестнадцати битными версиями БСШ [3,4]).

Рис. 1, заимствованный из описания mini-AES [2], иллюстрирует процесс шифрования сообщения с помощью нашей модели.

1.1. Компоненты шифра мини-Калина

Алгоритм ″Калина″ относится к Rijndael-подобным шифрам (как и AES, ADE), и поэтому для его описания удобно будет воспользоваться концепцией описания и терминологией, представленными в спецификации шифра mini-AES [2].

Для простоты описания процедуры шифрования входной 16-битный блок открытого текста P, состоящий из последовательности четырёх полубайтов $P=(p_0,p_1,p_2,p_3)$, представляется в виде матрицы размера 2×2, названной в соответствии с терминологией, использованной при описании шифра AES (и ADE), состоянием. Отмеченное представление иллюстрирует рис. 2.

Для представления полубайтов наряду с двоичной формой в дальнейшем будет использоваться и шестнадцатеричная форма представления, приведенная в табл. 1.

Итак, входной блок данных $p_0p_1p_2p_3$ представляется в виде матрицы-состояния $\begin{bmatrix} p_0 & p_2 \\ p_1 & p_3 \end{bmatrix}$.

Например, если входной блок 1000 1100 0111 0001 состоит из полубайтов $p_0=8$, $p_1=C$, $p_2=7$, $p_3=1$, то соответствующая матрица состояния будет иметь вид

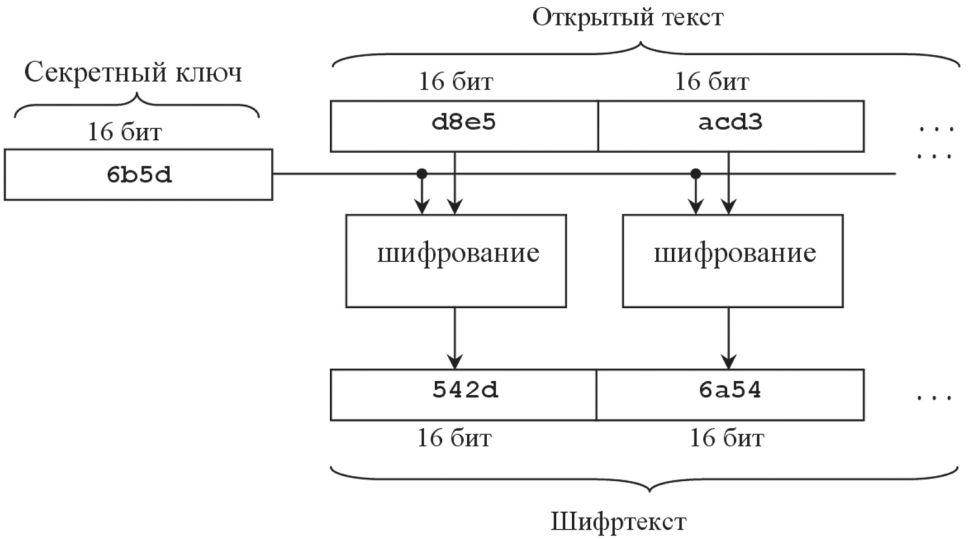


Рис. 1. Шифрование открытого сообщения БСШ с размером блока 16 бит

$$\begin{bmatrix} 8 & 7 \\ C & 1 \end{bmatrix}, \text{ или } \begin{bmatrix} 1000 & 0111 \\ 1100 & 0001 \end{bmatrix}.$$

Подобным же образом представляется и секретный ключ – как 4 полубайта $k_0k_1k_2k_3$ и соответствующее им состояние $\begin{bmatrix} k_0 & k_2 \\ k_1 & k_3 \end{bmatrix}$.

В процессе шифрования принимают участие пять основных компонент, а именно: операции *XORRoundKey, AddRoundKey, Sbox, ShiftRows* и *MixColumns,* многократное применение которых в определённом порядке и определяет процедуру шифрования. Еще одной важной частью шифра является алгоритм разворачивания ключа.

Цикл шифрования включает последовательное выполнение следующих преобразований:

– подстановка (Sbox);

– циклический сдвиг строк (ShiftRows);

– перемешивание в колонках (MixColumns);

– сложение с подключом по модулю 2^4 (AddRoundKey), если номер цикла четный и по модулю 2 (XORRoundKey), если номер цикла нечетный.

Перед повторением этих циклов производится сложение по модулю 2 с нулевым элементом массива подключей, а после цикловых преобразований – ещё одна подстановка (S-блок) и сложение по модулю 2^4 с последним элементом массива подключей. Количество циклов в оригинальной разработке равняется десяти, хотя в большинстве уменьшенных версий шифров оно равно четырём. Изменение этого параметра не составляет труда, поэтому в дальнейшем мы рассматриваем оба варианта реализации.

1.1.1. Сложение с ключом

Функции AddRoundKey и XORRoundKey достаточно просты, и полностью аналогичны тем, что использованы в оригинальной версии шифра.

1.1.2. Таблицы подстановок (Sbox)

В уменьшенной версии шифра Калина используются подстановки 16-го порядка. Они взяты из работы [3]:

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

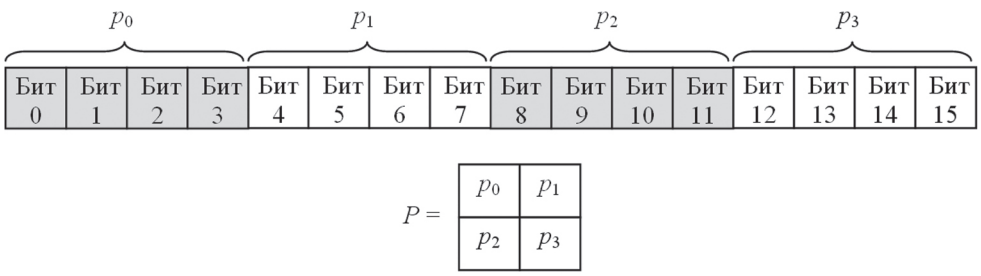


Рис. 2. Представление 16-битного блока в виде матрицы 2×2

Таблица 1

Представление 4-битных массивов в шестнадцатеричном виде

p-дв.	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
p-шестн.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Текущее состояние, как и в других функциях, представляется в виде массива полубайт размера 2×2.

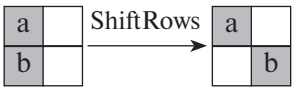
К первой строке массива применяется одна подстановка, ко второй – вторая.

Подстановка определяется как замена полубайта состояния на полубайт из таблицы, такой, что номер его столбца определяется двумя младшими, а строки – двумя старшими битами полубайта состояния. Достаточно очевидно, что если развернуть массив 4×4 по строкам в одномерный массив из шестнадцати полубайт, то подстановка определяется значительно проще: полубайт берётся просто по номеру в строке.

1.1.3. Циклический сдвиг строк (ShiftRows)

Ввиду того, что текущее состояние представлено в виде матрицы размером 2×2 полубайта, эта функция сильно вырождается относительно аналогичной в большом шифре.

Собственно при этом происходит только циклический сдвиг 2-й строки:



Из этого следует, что функция ShiftRows для уменьшенной версии будет обратной к самой себе, и создание отдельной функции invShiftRows не требуется.

1.1.4. Перемешивание в колонках (MixColumns)

Выполнение данной процедуры сводится к умножению матричного представления текущего состояния на константную матрицу над полем GF(2^4). В качестве константной использована матрица

10	7
7	15

Поле GF(2^4) задается полиномом $x^4 + x + 1$.

1.2. Инверсный шифр

Процедура расшифрования является обратной к процедуре зашифрования. Её код достаточно очевиден и пояснений не требует.

Функции XORRoundKey и ShiftRows являются инверсными в отношении самих себя, поэтому используются и при расшифровании.

Функции InvSbox и InvMixColumns аналогичны прямым, но используют другие встроенные данные, а именно:

S-блоки:

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

и матрицу:

3	5
5	2

Функция SubRoundKey, отличается от AddRoundKey знаком (выполняется модульное вычитание).

Последовательность применения данных функций представляет собой последовательность функций зашифрования, развёрнутую в обратном порядке с заменой функций зашифрования на обратные им (такой шифр называется инволютивным).

1.3. Схема разворачивания ключей

Для получения цикловых подключей из исходного мастер-ключа используется процедура разворачивания ключей. Для шифрования алгоритмом «мини-калина» необходимо 12 подключей, каждый длиной 4×4 бита (размер подключа совпадает с размером открытого/шифрованого текста и текущего состояния шифра).

Алгоритм разворачивания ключа работает по схеме, которая включает в себя два этапа:

1) На основе мастер-ключа и константы вырабатывается три ключевых состояния KS_{len}^{j}, где j – порядковый номер ключевого состояния, len – длина ключевого состояния в битах.

При этом константа складывается с мастер-ключом по модулю 2, а потом проходит два цикла шифрования (в первом она шифруется побитовой инверсией мастер-ключа, во второй – собственно мастер-ключом).

Для каждого ключевого состояния берётся своя константа.

Константы имеют вид:

$c_1 = \{1,1,1,1\}$;

$c_2 = \{2,2,2,1\}$;

$c_3 = \{3,3,3,1\}$;

2) на основе каждого из трёх KS_{len}^{j} с помощью циклических сдвигов вправо формируются цикловые подключи K_i.

Таблица 2 иллюстрирует процесс формирования цикловых подключей с помощью циклических сдвигов.

Таблица 2

Формирование подключей на основе циклических сдвигов

1	0	0	1	0	1	1	1	0	1	0	0	1	1	0	1	KS_{len}^{j}
0	1	1	0	1	1	0	0	1	0	1	1	1	0	1	0	>>5
1	0	0	1	1	0	1	1	0	0	1	0	1	1	1	0	>>7
1	1	1	0	1	0	0	1	1	0	1	1	0	0	1	0	>>11

Таким образом, мы получаем массив из шестнадцати цикловых подключей.

2. ИССЛЕДОВАНИЯ ЦИКЛИЧЕСКИХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «КАЛИНА»

При исследовании циклических свойств использована методика, изложенная в работе [6].

Если рассматривать шифр при заданном ключе как подстановку, определяющую переход от

исходного блока данных к зашифрованному (биективное отображение), то циклические свойства можно определить на основе результатов анализа последовательных зашифрований исходного текста на каждом ключе.

Здесь определяется закон распределения числа циклов для множества ключей зашифрования (подстановочных преобразований). Известно, что для случайных подстановок справедлива теорема [8].

Теорема. Если ξ_n – *число циклов равновероятно выбранной подстановки степени n, то случайная величина* $\xi_n' = \frac{\xi_n - \ln n}{\sqrt{\ln n}}$ *имеет в пределе нормальное распределение с параметрами* (0,1).

Мы сначала и поставили задачу оценки соответствия (близости) закона распределения числа циклов для множества ключей зашифрования шифра мини-Калина асимптотическому распределению.

2.1. Особенности программной реализации

Алгоритм работы программы такой: для каждого ключа из полного множества ключей мы производим поиск циклов и запоминаем получившееся их число. Поиск циклов производится так: мы создаём массив всех возможных вариантов пар исходный текст/зашифрованный текст и, начиная с нулевого элемента массива из заготовленных открытых тестов, применяем функцию шифрования, пока не обнаружим цикл (пока не придем снова к нулю). Таким образом, мы нашли цикл с нулевым образующим элементом, и в процессе пометили все элементы в него входящие. После этого мы выбираем наименьший элемент, не попавший в этот цикл, и строим новый цикл от него, также запоминая пройденные значения. Это мы повторяем до тех пор, пока все элементы массива исходных/зашифрованных текстов не попадут в один из циклов.

2.2. Результаты исследований циклических свойств и их анализ

Результат работы данной программы представляет собой файл достаточно большого размера, поэтому в табл. 3 представлена только его финальная часть. В таблице показаны также взятые из работ [3,4] результаты исследований уменьшенных моделей других шифров. Рассмотрены две версии уменьшенной модели шифра Калина: десятицикловый алгоритм (как в оригинальной версии) и четырёхцикловый (для сравнения с другими известными моделями). Из приведенных данных можно сделать вывод о том, что миниверсия шифра "Калина" практически повторяет циклические свойства других известных моделей шифров и, в частности, совпадает со свойствами шифра mini-AES. Соответственно процедуру шифрования данного шифра можно считать близкой к свойствам случайной подстановки. Из сравнения показателей десяти и четырехцикловой версий шифра видно, что появление ключа, порождающего 28 циклов, скорее является фактором случайности чем несовершенства алгоритма или реализации.

3. ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «КАЛИНА»

В процессе исследований были изучены также дифференциальные свойства подстановочных преобразований, формируемых мини шифром Калина. Некоторые результаты в этом направлении иллюстрирует табл. 4 (расчеты для шифра мини "Калина" выполнены по выборке из 10 ключей). В этой же таблице для сравнения представлены результаты изучения дифференциальных свойств малых версий блочных шифров Baby ADE и Mini AES, взятые из нашей работы [6] (данные получены по 1000-е ключам зашифрования).

Таблица 3

Сравнение циклических свойств уменьшенных моделей БСШ

Количество циклов	Количество подстановок Baby-Camellia	Количество подстановок Baby-Rijndael	Количество подстановок babyADE	Количество подстановок mini-Kalina (4 цикла)	Количество подстановок mini-Kalina (10 циклов)
2	28	18	32	2	27
4	496	499	521	549	507
6	3147	3255	3322	3167	3234
8	9373	9436	9415	9528	9482
10	15567	15429	15366	15256	15317
12	15903	15963	16124	15988	16054
14	11530	11580	11400	11760	11524
16	6168	5956	5952	5935	6052
18	2406	2411	2397	2384	2407
20	713	774	778	733	706
22	160	174	188	166	186
24	36	35	34	39	34
26	9	6	5	7	5
28	0	0	1	0	1
30	0	0	1	0	0

Таблица 4

Дифференциальные свойства мини шифра «Калина» при различном числе циклов шифрования

Шифр	Число циклов *r*						
	2	3	4	5	6	7	8
Baby ADE	3254±59	301,3±7,3	20,064±0,35	19,170±0,124	19,120±0,092	19,166±0,093	19,106±0,091
Mini AES	4955±24	640,6±4,6	43,066±0,99	20,538±0,202	19,082±0,093	19,122±0,092	19,122±0,096
Mini Калина	301±70	36,6±11,3	19,06 ±1	18,6±0,81	19,06±1,075	20±0,1	19,0±1

И в этом случае шифр рассматривается для каждого ключа зашифрования как подстановка порядка 2^{16} и таблица XOR разностей фактически представляет собой таблицу распределения полных дифференциалов шифра. Результаты свидетельствуют, что шифр ″Калина″ имеет показатели, не уступающие другим алгоритмам шифрования, представленным на Украинский конкурс.

Считаем важным также отметить, что полученные для малых моделей шифров (с числом циклов большим четырех) максимальные значения полных дифференциалов совпадают с ожидаемыми средними значениями максимумов таблиц XOR разностей случайных подстановок соответствующего порядка.

4. ИССЛЕДОВАНИЕ ЛИНЕЙНЫХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «КАЛИНА»

При исследовании линейных свойств мини версии шифра ″Калина″ была построена таблица линейных аппроксимаций размером $2^m \times 2^m$ для всего шифра, рассматриваемого как подстановка.

По принятой терминологии в этом случае значения такой таблицы называются линейным корпусом [7]. Полученные результаты вместе с данными аналогичного исследования, выполненного для шифра Лабиринт, представлены в табл. 3.

Следует здесь заметить, что объём вычислений при построении линейной аппроксимационной таблицы оказывается существенно большим, чем при определении максимума полного дифференциала. Он связан с битовым размером входа в шифр n как 2^{2n}, и выполнение полного объема расчетов даже для одного ключа и для 16-битных блоков данных оказывается вычислительно трудной задачей. Поэтому в табл. 5 иллюстрируются результаты вычислений для ограниченных наборов масок входа и выхода. В последнем случае объем выборки взят более, существенно меньшим, чем для первого шифра.

ЗАКЛЮЧЕНИЕ

Представленные результаты свидетельствуют, что шифр ″Калина″ обладает криптографическими показателями (из числа проверенных) не уступающими шифру Rijndael и другим шифрам, представленным на украинский конкурс по выбору кандидата на национальный стандарт симметричного блочного шифра.

Литература.

[1] *Горбенко І. Д, Долгов В.І., Олейніков Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Тоцкій О.С., Казьміна С.В.* Перспективний блоковий симетричний шифр “Калина” – основні положення та специфікації // Прикладна радіоелектроніка: наук.-техн. журнал. – 2007. Т.6. № 2. – С. 195-208.

[2] Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Tested for Cryptanalysis Students, Cryptologia, XXVI (4), 2002.

[3] *Долгов В.И., Кузнецов А.А., Сергеенко Р.В., Белоковаленко А.Л.* Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-Ade) // Прикладная радиоэлектроника: научн.-техн. журнал. – 2008. Т. 7. № 3. – С. 215-224.

[4] *Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В.* Исследование циклических и дифференциальных свойств уменьшенной модели шифра «Лабиринт». Прикладная радиоэлектроника: научн.-техн. журнал. – 2009. Т. 8. № 3. – С. 283-289.

[5] *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. Т.6, № 2. – С. 257-263.

[6] *Олейников Р.В., Лисицкая И.В., Широков А.В., Лисицкий К.Е.* Исследование дифференциальных свойств подстановок. Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. I, С. 59-63.

[7] *H. M. Heys.* A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002, p. 189-221.

[8] *Сачков В.Н.* Комбинаторные методы дискретной математики. – М.: Наука ,1977. – 319 с.

Поступила в редколлегию 7.07.2010.

Таблица 5

Линейные свойства шифров ″Лабиринт″ и ″Калина″

смещение	0	2	100	200	300	400	500	600	720
Линейный корпус шифра ″Лабиринт″									
количество	81839	163317	120328	48060	10378	1232	82	1	1
Линейный корпус шифра ″Калина″									
количество	29282	28825	21332	8522	1879	225	15	1	0

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Олейников Роман Васильевич, кандидат технических наук, докторант кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

Большаков Андрей Юрьевич, студент кафедры БИТ ХНУРЭ. Область научных интересов: анализ БСШ, статистические методы исследования стойкости.

Григорьев Андрей Владимирович, студент кафедры БИТ ХНУРЭ. Область научных интересов: анализ криптографических свойств блочных симметричных и потоковых шифров, и их схем разворачивания ключей.

Дроботько Екатерина Викторовна, магистр кафедры БИТ ХНУРЭ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров, анализ структурных элементов БСШ.

УДК 681.3.06

Криптографічні властивості зменшеної версії шифра «Калина» / В.І. Долгов, Р.В. Олійников, А.Ю. Большаков, А.В. Григорьєв, Е.В. Дроботько // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 349-354.

У роботі наведений опис зменшеної 16-бітової версії шифру «Калина» і результати дослідження декількох криптографічних показників зменшеної моделі (циклічні, диференційні, лінійні та інші властивості).

Ключові слова: симетричний блоковий шифр, випадкова перестановка.

Табл. 04. Іл.02. Бібліогр.: 08 найм.

UDC 681.3.06

Cryptographic properties of reduced version of «Kalina» cipher / V.I. Dolgov, R.V. Oleinikov, A.Yu. Bolshakov, A.V. Grigor'iev, E.V. Drobotko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 349-354.

The first part of the paper provides a description of the reduced cipher «Kalina» 16-bit version and the second one gives the results of researching a number of cryptographic indices of the reduced model (cyclic, differential, linear and other properties).

Key words: symmetric block cipher, random substitution.

Tab. 04. Fig. 02. Ref.: 08 items.

УДК 621.3.06

АТАКА НА ПОЛНЫЙ ДИФФЕРЕНЦИАЛ УМЕНЬШЕННОЙ ВЕРСИИ БСШ RIJNDAEL

В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, Д.Э. ХРЯПИН

Усовершенствуется поход к анализу показателей криптографической стойкости блочных симметричных шифров, строящийся на основе исследования свойств уменьшенных версий этих шифров. Излагаются некоторые результаты применения этой методики для решения задачи определения показателей стойкости шифров к атакам дифференциального криптоанализа. Предлагается решение задачи определения ключа зашифрования уменьшенной модели шифра Rijndael на основе выполнения атаки на полный дифференциал. Результаты обобщаются на оценки показателей стойкости больших шифров.

Ключевые слова: криптографическая стойкость, дифференциальный криптоанализ.

ВВЕДЕНИЕ

В эти дни в Украине проходит конкурс предложений по построению алгоритмов блочного симметричного шифрования, целью которого является отбор претендента на новый стандарт БСШ, взамен используемого до настоящего времени российского шифра ГОСТ 28149-87. Известно, по крайней мере, четыре предложения и сейчас идет их изучение заинтересованными организациями и специалистами.

Опыт показывает, что выполнение экспертизы современного блочного шифра и уровень ответственности при принятии решения является не простой задачей, требующей привлечения значительных временных и интеллектуальных ресурсов. Хотелось бы найти не только убедительные теоретические обоснования, найти которые в криптографии, как правило, очень непросто, но и получить реальные практические результаты, позволяющие собрать данные для сравнительного анализа претендентов. И здесь многие подходы сталкиваются практически во всех случаях с проблемой непреодолимой вычислительной сложности анализа современных БСШ.

Развивается точка зрения, что в значительной степени стоящие трудности можно преодолеть путем разработки и анализа криптографических свойств уменьшенных моделей кандидатов и сопоставления их показателей с показателями уменьшенных моделей известных шифров, которые уже поддаются проведению вычислительных экспериментов. Конечно, при этом необходимо позаботиться, чтобы в уменьшенных моделях были сохранены все основные преобразования и операции прототипов, т.е. чтобы обеспечивалась в известном смысле их ″эквивалентность″ большим прототипам. Некоторые результаты исследований в этом направлении мы уже публиковали в работах [1-4].

Мы хотим здесь напомнить выводы одной из последних наших работ [4], посвященных анализу экспериментов с уменьшенными моделями шифров, позволившему обосновать новую идеологию оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. Было установлено, что:

1. Современные блочные симметричные шифры (при полном наборе шифрующих многоцикловых преобразований) имеют свойства случайных подстановок и для них справедливы законы распределения вероятностей для полных дифференциалов и линейных корпусов свойственные таблицам дифференциальных разностей и линейных аппроксимаций случайных подстановок соответствующей степени. Но если этот результат представляется в некотором смысле ожидаемым, то остальные представляются далеко не очевидными.

2. Максимальные значения полных дифференциалов и линейных корпусов для современных БСШ, определяющие по современным меркам показатели стойкости шифров к атакам дифференциального и линейного криптоанализа, могут быть получены расчетным путем. Они не зависят (при достаточном числе цикловых преобразований ни от свойств используемых в шифрах подстановочных конструкций, ни от методов введения в цикловые функции цикловых подключей, ни от способа построения расширяющего линейного преобразования цикловой функции, а являются функцией только размера битового входа в шифр (порядка подстановки).

3. Для оценки стойкости блочных симметричных шифров с битовым размером входа равным n к атакам дифференциального и линейного криптоанализа справедливы приближенные расчетные соотношения [5, 6]

$$DP^{f}_{\max} = \frac{n+4}{2^{n}}$$

и

$$DL^{f}_{\max} = \left(\frac{\left(\frac{3}{2}\right)^{n}}{2^{n-1}} \right)^{2}.$$

Приведенные формулы позволяют, таким образом, оценить наибольшую вероятность полного дифференциала и линейного корпуса соответственно.

4. На основе анализа результатов проверки показателей стойкости уменьшенных моделей

шифров, представленных на украинский конкурс по выбору кандидата на национальный стандарт БСШ (7-10), сделан вывод, что все шифры, представленные на конкурс, имеют практически и теоретически одинаковые показатели стойкости к атакам дифференциального и линейного криптоанализа.

В соответствии с существующей точкой зрения максимальные значения дифференциальных и линейных вероятностей (максимальных вероятностей полных дифференциалов и линейных корпусов) непосредственно связаны со сложностью соответствующих криптоаналитических атак на шифры. Хотелось бы более глубоко осознать эту связь. Здесь возникает, по крайней мере, три вопроса, на которые хотелось бы получить ответы. Первый вопрос: если мы знаем характеристику (линейную или дифференциальную), соответствующую максимально вероятной, то можно ли на нее построить атаку и как? Конечно, же, найти максимально вероятную характеристику для большого шифра сама по себе сложная (возможно и невыполнимая) задача, но тогда можно искать не обязательно максимально вероятную, а заметно отличающуюся от многих других, и тогда спрашивается, какова вероятность найти такую (уменьшенную по сравнению с максимумом) характеристику? И, наконец, есть третий вопрос: имеется ли возможность выполнить атаку на шифр в случае, когда удается найти характеристику (дифференциальную или линейную), замыкающуюся на ограниченное число S-блоков первого или последнего циклов, которая имеет значение, существенно (а может и просто, заметно) превосходящее значения для многих других характеристик?

В этой работе мы попробуем ответить на эти вопросы, опять опираясь на результаты экспериментов с уменьшенными версиями шифров. И здесь мы будем возможность реализации на малые модели шифров атак переборного типа, что делает возможным в деталях познакомиться с особенностями и возможностями реализации таких атак и на большие шифры. В этой работе, в частности, внимание сосредотачивается на особенностях реализации атаки на полные дифференциалы уменьшенных моделей шифров Rijndael и SPN шифра из работы Хеуса. Естественно, что такого типа атаки на большие шифры до сих пор считаются не реализуемыми. Мы проверим истинность и этого предположения.

1. ПОСТРОЕНИЕ АТАКИ НА ПОЛНЫЙ ДИФФЕРЕНЦИАЛ SPN ШИФРА

Реализации малых шифров взяты из Интернета (для шифра Rijndael) и из ранее выполненных нами исследований и разработок [1-4], в основе которых лежат 16-битные модели.

Прежде всего, изложим саму сущность методики построения атаки на полный дифференциал. Вспомним работу Бихама и А. Шамира [5], в которой они описывают стратегию определения битов ключа на входе S-блока последнего цикла на основе анализа информации о прохождения разностей пар текстов через этот S-блок и знания значений самих текстов на входе расширяющей перестановки, предшествующей S-блоку. В рассматриваемом случае у нас нет значений выходов S-блока цикла (при расшифровании на один цикл зашифрованного текста), как это было в примере Э. Бихама и А. Шамира [5]. Поэтому нам остается только сделать ″откат″ на один цикл (расшифрование зашифрованных на неизвестном ключе пар текстов на одном из вариантов возможных ключей) и далее искать продолжение атаки, используя полученные значения разностей (теперь уже на входах S-блоков последнего цикла). И такая ситуация характерна для всех SPN шифров.

Обратим теперь внимание на то, что в итеративных многоцикловых шифрах последние циклы шифрующего преобразования (в сочетании с предыдущими циклами) ведут себя как случайные подстановки, т. е. фактически все входные биты предпоследнего цикла (более точно – последних циклов) являются активными (переходы разностей через последние циклы осуществляются без потери вероятностей в том смысле, что сохраняется закон распределения разностей переходов таблиц цикловых разностей [6]). Это означает, что для любого S-блока выходная разность формируется на основе полного набора возможных пар входов (для ключезависимой функции при сложении множества входов с ключевыми битами происходит перенаименование входов (они принимают новые значения) при сохранении распределения значений разностей между ними. В результате этого просто изменяется распределение выходов по выходным разностям. Поэтому следует считать одинаково (равновероятно) активными все возможные входные разности. Тогда, если мы рассматриваем какое-либо значение выходной разности S-блока последнего цикла (для пары, взятой из множества отобранных пар текстов с заданным значением разности), участвующего в формировании максимально вероятной дифференциальной характеристики, то естественно полагать, что при формировании этой наиболее вероятной характеристики используются переходы S-блока с наибольшими значениями.

Тогда значения выходов для инверсного S-блока (входов этого же S-блока при шифровании) для интересующей нас характеристики можно определить из таблицы XOR разностей задействованного S-блока, просто выбирая из нее значения, являющиеся наибольшими (таких значений может оказаться и не одно).

В результате рассматриваемая задача опять приводится к изложенной в работе [5], т. е. нам известны значения пар текстов с определенной разностью перед их сложением с ключевыми битами, после которого формируются входы в S-блок, а также известно значение разности на выходе S-блока.

И тогда полностью можно воспользоваться рассмотренной в работе [5] стратегией определения ключевых битов.

Перейдем теперь к результатам реализации изложенной стратегии построения атаки на полный дифференциал. Рассмотрим сначала SPN конструкцию в виде модели шифра подстановочно-перестановочной (SPN) структуры из работы [6], представленную на рис.1.

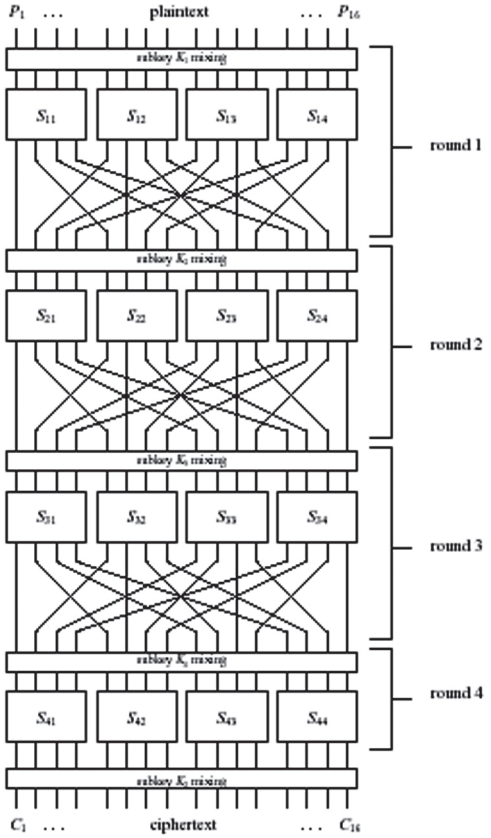


Рис 1. Шифр на основе подстановочно-перестановочной (SPN) структуры

В алгоритме в каждом отдельном цикле преобразований входной 16-битный блок данных делится на четыре подблока, каждый из которых поступает на соответствующие входы блоков замены (S-блоков, осуществляющих замену четырех входных битов на четыре выходных). Естественно, что каждый из блоков замены может быть представлен в виде таблицы, пример которой (мы следуем работе профессора X. Хеуса) представлен в табл. 1 (в данном случае S-блок представляет собой первую строку S-блока алгоритма шифрования DES). На рис.1 наиболее значимый бит шестнадцатеричных значений является самым левым битом выхода каждого S-блока.

Таблица 1

S-блок в шестнадцатеричной системе счисления

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

В нашем эксперименте использовано аналогичное нелинейное преобразование для всех S-блоков.

Таблица 2

Цикловые ключи

1	6	D	1
A	2	7	E
3	9	7	F
F	7	C	6
2	9	0	2

Первым этапом задачи стал поиск максимально вероятной дифференциальной характеристики (полного дифференциала). В нашем эксперименте за основу была взята процедура расшифрования (хотя с одинаковым успехом можно было бы взять и процедуру зашифрования). Для поиска полного дифференциала использовалась та же методика, что и при построении таблиц дифференциальных разностей подстановок [5] (последовательно перебирались пары текстов с фиксированной входной разностью, и подсчитывалось число пар входов с фиксированной входной разностью, которые при расшифровании формировали одну и ту же выходную разность).

После выполнения 4-х цикловой программы с вышеописанными параметрами были получены результаты (для отдельного фиксированного значения мастер-ключа зашифрования при вариации по всему множеству 2^{16} пар текстов для каждой входной разности), представленные в таблице 3.

Таблица 3

Результаты поиска максимально вероятного дифференциала для 4-х циклового шифра

Входная разность (hex)	0505	5415	BB0B
Выходная разность (hex)	B0BB	B0B0	E0A0
Количество повторов (dec)	216	186	44

Для поиска частного (из множества полных) дифференциала (частного в смысле анализа не полного множества дифференциалов, т.е. речь здесь снова шла о полных дифференциалах) использовался фактически тот же алгоритм, только объем вычислений был существенно сокращен (до 2^4 пар текстов). Кроме того, в отличие от первого случая, зашифрование проводилось уже на 8-ми циклах. S-блоки остались прежними (одинаковыми). Цикловые (раундовые) ключи были расширены [см. табл. 4]

Таблица 4

Расширенные цикловые ключи

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

Результаты, полученные после выполнения программы с указанными параметрами, представлены в таблице 5.

Таблица 5

Результаты выполнения поиска максимально вероятного дифференциала

Входная разность (hex)	7	1	2
Выходная разность (hex)	6583	C890	1FF8
Количество повторов (dec)	12	10	10

Из результатов измерений, представленных в таблицах 3 и 5, следует, что максимально достижимые значения полных дифференциалов для шифра с четырьмя циклами существенно отличаются от соответствующих значений шифра с 8-ю циклами. Это следует и из нашей работы [2 и др.]. Напомним, что как показано в работе [2], SPN шифр рассмотренного типа выходит на ″асимптотические″ значения полного дифференциала (становится случайной подстановкой) лишь при 7-8-ми циклах, в то время как уменьшенная модель шифром Rijndael приходит к потенциальному значению максимума полного дифференциала уже при 4-х циклах.

2. РЕАЛИЗАЦИЯ АТАКИ КРИПТОАНАЛИЗА

Для атаки использовали следующий алгоритм.

Выполняется дешифрование пар шифртекстов, входящих в отобранные пары (реализующие один из выделенных в таблицах переходов) на цикл (раунд) на всех возможных множествах значений ключевых битов, участвующих в формировании выходной (после одноциклового расшифрования) разности (на входе инверсных S-блоков). Затем с помощью счетчиков определяется, для какого из сочетаний ключевых битов получаемые значения разностей совпадают наибольшее число раз с разностями (разностью) на входах (входе) S-блоков (S-блока), следующими (следующей) из таблицы 6.

В данном случае для выходной разности 6583 следует считать наиболее вероятным переходом слоя для S-блоков последнего цикла входную разность 84F1. Результаты выполнения атаки на полный дифференциал (на весь шифр) иллюстрирует таблица 7 естественно, что атака начинается с перехода с максимальной вероятностью.

Таблица 7

Результаты выполнения атаки на полный дифференциал (всего шифра)

Входная разность 4 цикл (hex)	505	5415	BB0B	0066	0B0B
Выходная разность 3 цикл (hex)	202	808	8088	0660	2022
Количество ключей до цикла поиска (dec)	65536	1024	256	16	4
Количество ключей после цикла поиска (dec)	1024	256	16	4	1

Заметим, что при использовании только одной разности не удается достичь однозначного определения подключа последнего цикла (максимальное значение подтверждает множество возможных подключей). Поэтому атака продолжается с использованием множества пар текстов, удовлетворяющих очередной из отобранных пар разностей.

Результаты выполнения атаки на ″частный дифференциал″ иллюстрирует табл. 8

Таблица 8

Результаты и параметры атаки на ″частный дифференциал″

Входная разность 8 цикл (hex)	7	1	2
Выходная разность 7 цикл (hex)	D	D	A
Количество ключей до цикла поиска (dec)	16	4	2
Количество ключей после цикла поиска (dec)	4	2	1

Таблица 6

Дифференциальная характеристика S-блока

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

На рис. 2 представлена сравнительная диаграмма, иллюстрирующая процесс устранения неопределенности с использованием 3-х возможных разностей.

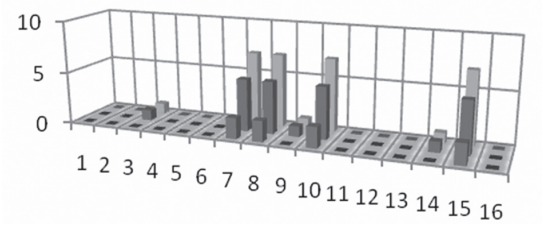


Рис. 2. Сравнительная диаграмма устранения неопределенности с использованием трех возможных разностей

В результате видно, что искомая разность третья, а вероятные ключевые биты (полубайты) 7,8,10,15 (7,8,A,F_h).

Криптоанализ уменьшенной 8-цикловой модели шифра Rijndael.

Мы здесь воспользовались уже имеющейся в Интернете разработкой уменьшенной модели шифра Rijndael [8], только число циклов было увеличено до 9-ти (8-мь и последний цикл неполный).

Для проведения дифференциального криптоанализа и в этом случае сначала изучались частные дифференциальные характеристики, начиная с минимального размера входного блока данных (полубайта), с дальнейшим увеличением размера входного блока до байта.

В качестве ключа использовали следующую таблицу, полученную при помощи алгоритма разворачивания ключей, описанного в [3].

Таблица 9

Последовательность цикловых подключей алгоритма зашифрования baby Rijndael

№ цикла	Ключ			
0	1	2	3	4
1	1	0	2	1
2	4	5	5	7
3	2	6	3	6
4	8	A	C	F
5	7	F	5	9
6	A	D	2	7
7	3	9	4	6
8	1	2	B	F
9	A	B	9	2

При анализе каждого из возможных 4-х битных блоков результат был одинаковый: максимальное значение – это 2 (симметричные) пары текстов, которые дают одинаковое значение выходной разности. При активации 2-ух (правых) S-блоков для 24 дифференциалов на выходе алгоритма шифрования нашлось 4 пары текстов, которые дали одинаковые значения выходной разности (на входе алгоритма шифрования). Ниже перечислены значения дифференциалов на выходе шифра при активации 2 левых S-блоков:

02, 08,13, 1B, 47, 55, 66, 68, 6A, 6B, 88, 9F, A4, A6, A9, AB, B8, B, CD, CF, D0, D4, F4, FC.

При активации 2 левых S-блоков появился один точный максимум для пары разностей Δx = 082C, Δy = 0300. Количество пар текстов удовлетворяющих этой разности равно 6. Эти тексты приведены в таблице 10.

На втором этапе, методом перебора всех ключей, в рабочем диапазоне (2^8), выбираются те, которые дают промежуточную дифференциальную характеристику (на входе последнего S-блока) совпадающую с характеристикой, полученной при анализе таблицы переходов S-блоков.

Таблица 10

Пары текстов с выходной разностью 6

№ пары	Пара текстов	
1	1400	1700
2	1700	1400
3	4C00	4F00
4	4F00	4C00
5	A500	A600
6	A600	A500

Исследуемое выходное значение разности равно 3. По таблице определяем, что вероятней всего на входе S-блока значение разности будет 6 или E. Проведем поиск ключей устраивающих обе пары разностей. Оба поиска отобразим на рисунке ниже.

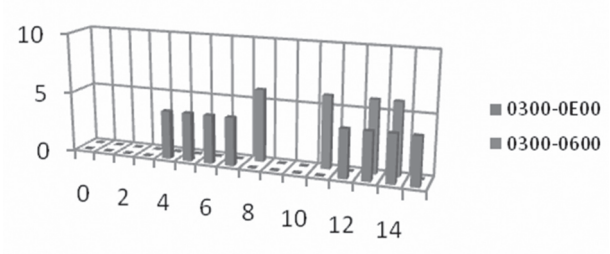


Рис. 3. Сравнительная диаграмма устранения неопределенности с использованием двух возможных разностей

Из рисунка видно, что правильным значением промежуточной разности является 6. Из рисунка также видно, что из 16 возможных ключей (фактически мы все-таки задействовали всего 1 S-блок) осталось только 4. Для продолжения криптоанализа, повторили 2 этап, но для другой разности (число текстов для новой пары разностей уже может быть меньше, но от него зависит качество отсеиваемых ключей). В дальнейшем для уточнения ключа использовались следующие пары:

$$\Delta x = \text{CD57} \rightarrow \Delta y = 0100;\ n = 4\ \Delta z = 0500,$$
$$\Delta x = \text{ABAA} \rightarrow \Delta y = 0\text{F}00;\ n = 4\ \Delta z = 0300.$$

Двукратное повторение 2 этапа позволяет уменьшить количество возможных ключей до 2-х (xBxx, xCxx). В результате общее количество возможных ключей сократилось с 256-ти до 32-х (т.е. в 8 раз). Дальнейшее сокращение количества возможных ключей было выполнено за счет оп-

ределения других байтов ключа Для определения старшего байта ключа, необходимо выбрать такую пару разностей, у которой 2-й байт на выходе алгоритма шифрования будет отличен от 0.

ЗАКЛЮЧЕНИЕ

Общим итогом работы является обоснование и демонстрация принципов реализации атаки на полный дифференциал SPN шифра.

Самый главный результат состоит в том, что атака дифференциального криптоанализа на блочный итеративный шифр может быть построена и на значение полного дифференциала существенно меньшее, чем максимальное значение полного дифференциала, на которое ориентируются при оценке стойкости блочных шифров.

В результате мы приходим к выводу, что все ж совсем не маловажное значение в возможности осуществления атаки дифференциального криптоанализа на SPN шифр играют дифференциальные свойства S-блоков. Они должны быть выбраны так, чтобы таблица XOR разностей не имела существенных отличий от среднего значения случайной подстановки.

От этого, правда, не меняется результирующий закон распределения разностей (полных дифференциалов) преобразования. И поэтому все равно будут существовать выбросы (значения переходов), которые можно пытаться использовать для атак.

Литература.

[1] *Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В.* Исследование циклических и дифференциальных свойств уменьшенной модели шифра "Лабиринт". // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2009. Т. 8, № 3, С. 283-289.

[2] *Долгов В. И., Лисицкая И. В., Киянчук Р. И.* Rijndael – это новое или хорошо забытое старое? Сборник трудов Первой Международной научно-технической конференции "Компьютерные науки и технологии", 8-10 октября 2009г., Белгород, Ч. II, С. 32-35.

[3] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Олешко О.И.* Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES // Прикладная радиоэлектроника. – 2009. – Т.8 – №.3, С. 252-257.

[4] *Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д.* Дифференциальные свойства случайных подстановок. // Прикладная радиоэлектроника. – 2010. Т. 9, № 3. – С. 326-333.

[5] Eli Biham, Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystem, Journal of Cryptology, Vol. 4, 1991. pp.3-72.

[6] *Горбенко И.Д., Долгов В.И., Лисицкая И.В, Олейников Р.В.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. // Прикладная радиоэлектроника. – 2010. Т. 9, № 3. – С. 312-320.

[7] *Horst Feistel.* Cryptography and Computer Privacy // Scientific American. – May 1973. – Vol. 228, No.5. – pp. 15-23.

[8] A Description of Baby Rijndael. ISU CprE/Math 533; NTU ST765-U February 19, 2003.

Поступила в редколлегию 9.07.2010.

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Хряпин Дмитрий Эдуардович, студент кафедры БИТ ХНУРЭ. Область научных интересов: криптоаналитические свойства БСШ, симметричные криптосистемы и протоколы.

УДК 621.3.06

Атака на повний диференціал зменшеної версії БСШ Rijndael / В.І. Долгов, І.В. Лисицька, Д.Е. Хряпін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 355–360.

Удосконалюється підхід до аналізу показників криптографічної стійкості блочних симетричних шифрів, побудованих на базі дослідження якостей зменшених версій цих шифрів. Викладаються деякі результати застосування цієї методики для рішення задачі визначення показників стійкості шифрів до атак диференційного криптоаналізу. Пропонується рішення задачі визначення ключа шифрування зменшеної моделі шифру Rijndael на базі виконання атаки на повний диференціал. Результати узагальнюються на оцінки показників стійкості великих шифрів.

Ключові слова: криптографічна стійкість, диференціальний криптоаналіз.

Табл. 10. Іл.03. Бібліогр.: 08 найм.

UDK 621.3.06

Attack on the full differential of reduced version of block symmetric cipher Rijndael / V.I. Dolgov, I.V. Lisitskaya, D.A. Hryapin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 355-360.

An approach to analyzing the properties of the cryptographic stability of block symmetrical ciphers, which is formed on the base of researching characteristics of the reduced version of these ciphers is improved. Some results of using these methods for solving the problem of determining the indices of the strength of ciphers to differential cryptanalysis attacks are given. A solution to the problem of determining the encryption key of the reduced cipher Rijndael model on the basis of performing a full differential attack is suggested. Results are generalized on estimations of the strength indices of big ciphers.

Key words: cryptographic strength, differential cryptanalysis.

Tab. 10. Fig. 03. Ref.: 08 items.

УДК 621. 391:519.2:519.7

КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ БЛОЧНЫХ ШИФРОВ ПРИ ИСПОЛЬЗОВАНИИ РАЗЛИЧНЫХ ОПЕРАЦИЙ СЛОЖЕНИЯ С ПОДКЛЮЧАМИ

В.И. РУЖЕНЦЕВ, В.В. СТУПАК

Исследуется криптографическая стойкость блочных симметричных шифров при использовании для введения секретности операций сложения по разным модулям. Рассматривается стойкость к дифференциальным, линейным, алгебраическим и другим атакам.

Ключевые слова: блочный симметричный шифр, криптографическая стойкость.

ВВЕДЕНИЕ

В соответствии с общеизвестными принципами Шеннона современные блочные симметричные шифры (БСШ) содержат операции перемешивания, рассеивания и операции введения секретности. В качестве операций перемешивания обычно используются подстановки, функции рассеивания возлагаются на линейные преобразования, а для введения секретности обычно используют сложение по XOR с подключом. Однако известны шифры, в которых для сложения с подключами используется не одна, а несколько операций сложения. К таким, например, относятся шифры семейства SAFER [1], а также представленные на национальный конкурс блочные шифры Калина [2], Лабиринт [3]. Целью данной работы является изложение результатов исследования криптографической стойкости блочных шифров при использовании в них операций сложения по разным модулям.

1. ОПИСАНИЕ РАССМАТРИВАЕМЫХ УМЕНЬШЕННЫХ МОДЕЛЕЙ

В рамках проведенных исследований рассматривались криптографические свойства фейстель-подобных и SPN блочных шифров с уменьшенным размером блока и ключа (8 или 16 битов). Целесообразность рассмотрения именно уменьшенных моделей шифров объясняется тем, что для изучения стойкости шифра к дифференциальной и линейной атаке следует, соответственно, оценивать вероятности полных дифференциалов и вероятности линейных корпусов – параметры, которые можно оценить только для шифра с небольшим размером блока. В качестве операций перемешивания и рассеивания были взяты преобразования, предложенные в [4] для уменьшенной версии шифра Rijndael. На рис. 1 и 2 схематически представлены преобразования, которые выполняются в рассматриваемых моделях фейстель-подобных и SPN шифров.

Исследованию криптографических свойств уменьшенных моделей блочных шифров посвящены и другие наши работы [5,6]. К основным особенностям предложенных уменьшенных моделей шифров следует отнести:

– размер блока 16 бит, размер ключа 8 или 16 бит;

– структура блока для SPN: 2 колонки по 2 4-битовых элемента;

– структура полублока для фейстель-подобного: 2 4-битовых элемента;

– умножение элементов каждой колонки на фиксированную МДР-матрицу размером 2 на 2 над $GF(2^4)$ (MixColumns);

– подстановка 4 в 4 бита (SubBytes);

– число ветвей активизации линейного преобразования MixColumns B = 3.

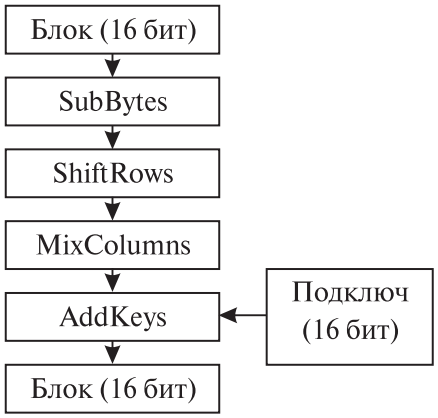


Рис. 1. Схема одного цикла SPN-шифра

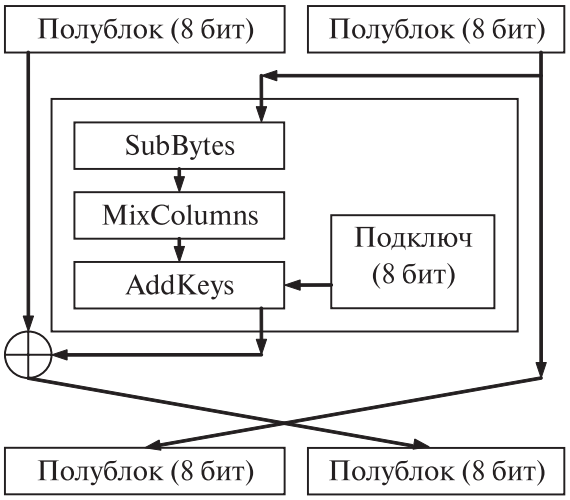


Рис. 2. Схема одного цикла фейстель-подобного шифра

2. СТОЙКОСТЬ К ДИФФЕРЕНЦИАЛЬНОМУ КРИПТОАНАЛИЗУ

Методика проверки точного критерия стойкости БСШ к дифференциальному криптоанализу сводится к оценке максимальных вероятностей дифференциалов. Для шифра с небольшим размером блока процесс поиска максимальных вероятностей дифференциалов похож на алгоритм построения таблиц разностей для подстановок, формируемых шифром при использовании различных ключей, и заключается в выполнении следующих шагов:

1. Перебираем значения ключа (100 значений).
2. Строим таблицу разности. Перебираем все значения входной разности (2^{16}).
3. Перебираем все значения одного из плайнтекстов (2^{16}).
4. Определяем выходную разность.
5. Определяем вероятности получения каждой выходной разности.
6. Определяем максимальную вероятность предсказания выходной разности
7. Определяем ожидаемое значение максимальной вероятности, усредняя значения, полученные на разных ключах.

Известны теоретические оценки ожидаемого значения максимальной вероятности дифференциала для случайной подстановки (см. представленную в этом же журнале статью «Дифференциальные свойства случайной подстановки»). Для случайной подстановки 16 в 16 битов математическое ожидание максимального значения в таблице разности составляет 19. Кроме того, из [6] известно, что для итеративного шифра при достижении некоторого количества циклов этот параметр перестает изменяться. Поэтому в итоговой таблице 1 приведено минимальное количество циклов, при котором шифры достигают теоретически ожидаемого максимума в таблице разности.

Таблица 1

Шифры (блок 16 битов)	Мин. число циклов для достижения теорет. ож. значения максим. вероятности дифференциала
SPN xor	5
SPN add	5
SPN add xor	5
FN xor	8
FN add	8
FN add xor	8

В табл. 1 и последующих таблицах использованы следующие обозначения:

SPN, FN – соответственно, SPN-шифр и фейстель-подобный шифр;

xor – в качестве операции сложения с подключом используется XOR;

add – в качестве операции сложения с подключом используется сложение по модулю 2^{16} для SPN и сложение по модулю 2^8 для фейстель-подобных шифров;

add xor – операции чередуются по циклам шифрования.

3. СТОЙКОСТЬ К ЛИНЕЙНОМУ КРИПТОАНАЛИЗУ

При оценке стойкости шифра к линейному криптоанализу следует проверять теоретический или точный критерий, то есть оценивать вероятности линейных корпусов (linear hull) (ЛК). Этот показатель может быть вычислен только для шифров с небольшим размером блока.

Процесс поиска ЛК, обладающего высокой вероятностью, похож на процесс построения таблицы линейных аппроксимаций для подстановки, образуемой шифром. Для получения значения вероятности ЛК необходимо произвести анализ вероятности ЛК для всех значений ключа, однако практическое решение такой задачи требует достаточно высоких вычислительных затрат. В ходе эксперимента вероятности ЛК оценивались только для одного ключа (все биты равны 0) и для ограниченного набора входных масок (от 1_{16} до 8_{16}).

Разработан и реализован алгоритм поиска максимальных вероятностей ЛК для масштабированных моделей различных БСШ с различным числом циклов.

Известны теоретические оценки ожидаемого значения максимальной вероятности ЛК для случайной подстановки (см. представленную в этом же журнале статью «Свойства таблиц линейной аппроксимации случайной подстановки»). Для случайной подстановки 16 в 16 битов математическое ожидание максимального значения в таблице линейной аппроксимации составляет около 620. Для итеративного шифра при достижении некоторого количества циклов этот параметр перестает изменяться. Поэтому в итоговой таблице 2 приведено минимальное количество циклов, при котором шифры достигают теоретически ожидаемого максимального значения в таблице линейной аппроксимации.

Таблица 2

Шифры (блок 16 битов)	Мин. число циклов для достижения теорет. ож. значения максим. вероятности лин. аппроксимации
SPN xor	4
SPN add	4
SPN add xor	4
FN xor	7
FN add	6
FN add xor	7

4. ЦИКЛИЧЕСКИЕ СВОЙСТВА ШИФРОВ

С групповыми (циклическими) свойствами шифрующих преобразований связано и одно из важных свойств блочного шифра, используемого в режиме счетчика или в режиме с обратной свя-

зью по выходу (OFB) – значение периода гаммы шифрующей, влияющего на выбор системных характеристик соответствующего профиля защиты информации.

Предлагается подход к анализу циклических свойств шифрующих преобразований, основанный на использовании предположения о принадлежности подстановок, порождаемых БСШ, к числу подстановок случайного типа. В литературе были найдены теоретические оценки показателей, характеризующих циклические свойства подстановок. В том числе, случайная подстановка 16 в 16 битов обладает следующими параметрами:

– математическое ожидание количества циклов: 12;

– максимальное количество циклов при рассмотрении 2^{16} случайных подстановок: 26.

Для каждого из рассматриваемых шифров экспериментальным путем было определено количество циклов преобразований, при котором формируемая шифром подстановка обладает свойствами случайной подстановки. Полученные результаты представлены в табл. 3.

Таблица 3

Шифры (блок 16 битов)	Мин. число циклов для достижения теорет. ож. значений циклических параметров
SPN xor	3
SPN add	3
SPN add xor	3
FN xor	7
FN add	5
FN add xor	5

Анализируя полученные результаты следует заметить, что использование модульного сложения в качестве операции введения секретности позволяет улучшить циклические свойства фейстель-подобных шифров, однако не влияет на свойства SPN шифров.

5. СТОЙКОСТЬ К ИНТЕРПОЛЯЦИОННОЙ АТАКЕ И АТАКЕ ЛИНЕЙНЫХ СУММ

В работе [7] предложен алгоритм, позволяющий оценить стойкость шифра к атаке линейных сумм и интерполяционной атаке. На практике этот алгоритм реализуем для случая, когда строящийся полином $f_k(x)$ связывает значения одного байта открытого текста с одним байтом шифртекста. Полином $f_k(x)$ имеет следующий вид:

$$f_k(x) = \sum_{i=1}^{2^8} a_i(k) b_i(x),$$

где $x \in GF(2^8)$ – байт открытого текста, $a_i(k) \in GF(2^8)$ – ключезависимые коэффициенты, $\{b_i(x)\}$ – множество линейно независимых полиномов с коэффициентами из $GF(2^8)$ (атака линейных сумм эквивалентна интерполяционной атаке, когда $b_i(x) = x^{i-1}$).

Атака линейных сумм эффективна, когда N, число неизвестных ключезависимых коэффициентов $a_i(k)$, меньше, чем 2^8.

Алгоритм для оценки количества ключезависимых коэффициентов N из [7] был реализован и с его помощью был произведен поиск количества ключезависимых коэффициентов в полиномах, связывающих байты открытого текста и байты криптограмм для SPN- и фейстель-подобных шифров с размером блока 128 битов (шифры имеют такую же структуру преобразований, как на рис.1 и 2, отличие в размерах блока (128 битов) и подключа (128 и 64 бита)). Результаты тестирования представлены в табл. 4.

Таблица 4

Шифры (блок 128 битов)	Мин. число циклов для обеспечения стойкости к интерполяционной атаке
SPN xor	3
SPN add	2
SPN add xor	2
FN xor	5
FN add	4
FN add xor	4

ВЫВОДЫ

Максимальные вероятности дифференциалов и линейных корпусов для SPN- и фейстель-подобных шифров не зависят от используемых операций введения секретности. Чередование нескольких операций сложения также не оказывает существенного влияния на значения указанных параметров.

Использование нескольких операций введения секретности позволяет улучшить циклические свойства и повысить стойкость шифра к алгебраическим атакам, таким как интерполяционная атака и атака линейных сумм. Но и в этом случае выигрыш составляет не более одного цикла преобразований как для SPN-, так и для фейстель-подобных шифров.

Литература:

[1] *J.L. Massey,* «SAFER K-64: A byte-oriented block-ciphering algorithm», R. Anderson, editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 1–17, SpringerVerlag, 1994.

[2] *Горбенко І.Д., Долгов В.І., Олійников Р.В., Руженцев В.І. та інші.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація» // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. Том. 6. № 2. – С. 195-208.

[3] *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. Том. 6. № 2. – С. 230-240.

[4] *E. Kleiman.* The XL and XSL attacks on Baby Rijndael. Thesis, 2005, available from http://orion.math.iastate.edu/dept/thesisarchive/MS/EKleimanMSSS05.pdf.

[5] *Долгов В.И., Руженцев В.И.* «Сравнительный анализ криптостойкости уменьшенных моделей блочных шифров» // Праці міжнар. симпозіуму «Питання оптимізації обчислень» (ПОО), 24-29 вересня 2009. Київ: Інститут кібернетики ім. Глушкова НАН України, 2009. Т.1. С. 211-215.

[6] *Долгов В.И., Руженцев В.И., Олейников Р.В.* Дифференциальные свойства масштабированных моделей блочных симметричных шифров, 11-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах», 20-23 мая 2008. Тезисы докладов. – К.: ЧП «ЕКМО» НИЦ «ТЕЗИС» НТУУ «КПИ», 2008.

[7] *K. Aoki.* Practical Evaluation of Security against Generalized Interpolation Attack. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan), Vol. E83-A, No. 1, pp. 33–38, 2000. (A preliminary version was presented at SAC'99).

Поступила в редколлегию 9.07.2010.

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров.

Ступак Валерий Владимирович, начальник отдела НКАУ, соискатель кафедры БИТ ХНУРЭ. Область научных интересов: криптография, системы защиты информации, криптоанализ блочних симметричных шифров.

УДК 621. 391:519.2:519.7

Криптографічна стійкість блокових шифрів при використанні різних операцій додавання з підключами / В.І. Руженцев, В.В. Ступак // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 361-364.

Досліджується кріптографічна стійкість блокових симетричних шифрів при використанні різних операцій додавання підключей. Досліджується стійкість до диференційних, лінійних, алгебраїчним та іншим атакам.

Ключові слова: блоковий симетричний шифр, криптографічна стійкість.

Табл. 4. Іл. 2. Бібліогр.: 7 назв.

UDC 621. 391:519.2:519.7

Cryptographic strength of block ciphers with using different sub-key addition operations / V.I. Ruzhentsev, V.V. Stupak // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 361-364.

The paper investigates the cryptographic strength of block symmetric ciphers with using different sub-key addition operations. The strength to differential, linear, algebraic and other attacks is considered.

Key words: symmetric block cipher, cryptographic strength.

Tab. 4. Fig. 2. Ref.: 7 items.

МЕТОДЫ, МЕХАНИЗМЫ И ПРОТОКОЛЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.3.06

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО МАКСИМАЛЬНЫМ КРИВЫМ ГУРВИЦА

Г. З. ХАЛИМОВ

Представлены результаты исследований по максимальным кривым Гурвица для целей универсального хеширования, условия максимальности обобщенных кривых, максимальная кривая Гурвица с третьим значением рода.

Ключевые слова: универсальное хеширование, кривые Гурвица.

ВВЕДЕНИЕ

Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на границе Хассе-Вейля. Основные результаты по кривым Гурвица представлены в работах F.Torres [1,2], также в работах[3,4]. Связь между кривыми Гурвица и Ферма представлена P. Carbonne, T.Henocq в [3]. В работе [1] введено определение обобщенных кривых Гурвица и установлен морфизм между обобщенными кривыми Гурвица и Ферма. Здесь же определены условия максимальности для обычных кривых Гурвица и обобщенных кривых при ограничении на выбор показателей степени кривой. Оценки числа решений кривой Гурвица для произвольного конечного поля и частные результаты по оценкам представлены в [4]. Теорема о существования нетривиальных кривых Гурвица и правила построения нетривиальных кривых также получены в [4].

Целью статьи является определение условий максимальности кривых Гурвица без ограничений на показатели степени кривой. В разделе 1 приводятся определение и свойства универсального хеширования в поле рациональных функций по точкам алгебраической кривой. В разделе 2 представлены определение и свойства кривых Гурвица, в разделе 3 – результаты по построению максимальных кривых Гурвица и оценке параметров.

1. УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ В ПОЛЕ РАЦИОНАЛЬНЫХ ФУНКЦИЙ

Универсальное хеширование в поле рациональных функций по точкам алгебраической кривой впервые введено Биербрауэром [5]. Интерпретация алгеброгеометрического подхода излагается в работах [4, 6].

Определение 1 [6]. Пусть задана абсолютно неразложимая, несингулярная проективная кривая χ над полем F_q с точками $P=\{P_1,P_2,...,P_n\}\in\chi(F_q)$. Для каждой алгебраической кривой можно определить поле рациональных функций $F_q(\chi)$. В каждой точке P_j кривой χ можно вычислить оценку ϑ_P для рациональных функций $f_i\in F_q(\chi)$, которая определяет порядок нуля или полюса функции f_i в этой точке. Хеш значение $h_{P_j}(m)\in F_q$ для сообщения $m=(m_1, m_2, ..., m_k)$, $m_i\in F_q$ в точке $P_j\in F_q$ определяется выражением

$$h_{P_j}(m)=\sum_{i=1}^{k} f_i(P_j)m_i\ , \qquad (1)$$

где $f_i\in F_q(\chi)$ с упорядоченными порядками полюсов $0<u_1<u_2< ...<u_k$. Хеш функция $h_{P_j}(m)$ определяет универсальный хеш класс $\varepsilon-U(N,q^k,q)$, где вероятность коллизии $\varepsilon\le u_k/N$, N – число точек алгебраической кривой.

Проблематика построения схем универсального хеширования на основе алгеброгеометрического представления заключается в выборе алгебраических кривых с требуемыми параметрами. Интерес представляют алгебраические кривые с как можно большим отношением числа точек кривой к её роду, определенные над конечным полем F_q. Наилучший результат универсального хеширования достигается на максимальных кривых [2]. Классическими максимальными кривыми являются кривые Эрмита, Сузуки, Делигнэ-Лустига. Lachaud G в [7] показал, что если кривая покрывается максимальной кривой, то она также является максимальной.

Предложение 1. [7] Пусть X_1 и X_2 неприводимые алгебраические кривые, определенные в проективном пространстве над полем F_q. Предположим, что существует морфизм $f: X_1\to X_2$ над полем F_q. Тогда если X_1 является максимальной кривой, тогда максимальной кривой является X_2.

Этот замечательный результат позволяет расширить поиск максимальных кривых Гурвица.

2. ОПРЕДЕЛЕНИЕ И СВОЙСТВА КРИВЫХ ГУРВИЦА

Кривые Гурвица H_n определяются выражением

$$X^nY+Y^nZ+XZ^n=0 \qquad (2)$$

и имеют частные производные вида $F_X=nX^{n-1}Y+Z^n$, $F_Y=nY^{n-1}Z+X^n$, $F_Z=nZ^{n-1}X+Y^n$.

Существует обобщение кривых Гурвица $H_{n,l}$, которое имеет вид

$$X^nY^l + Y^nZ^l + X^lZ^n = 0, \quad (3)$$

где $n \geq l \geq 2$ и $\Delta(n, l) = n^2 - nl + l^2 \geq 2$.

Между кривыми Гурвица и Ферма существует морфизм, установленный P. Carbonne, T.Henocq в [3] и определенный в лемме 1.

Лемма 1. Кривая Гурвица H_n является F_q покрытой кривой Ферма

$$U^{n^2-n+1} + V^{n^2-n+1} + W^{n^2-n+1} = 0.$$

Известно обобщение леммы 1 для кривых Гурвица общего вида F.Torres в [1].

Лемма 2. Кривая Гурвица $H_{n,1}$ является F_q покрытой кривой Ферма

$$U^{n^2-nl+l^2} + V^{n^2-nl+l^2} + W^{n^2-nl+l^2} = 0.$$

Следующее утверждение является новым и определяет семейства нетривиальных кривых Гурвица, число точек которых не равно размерности поля.

Утверждение 1. Пусть F_q конечное поле и $q-1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $e_i \geq 1$. Нетривиальные кривые Гурвица $\mathcal{H}_{n,l}$ принадлежат одному из семейств:

a) $X^nY + Y^nZ + XZ^n = 0$,

если $\Delta(n,l=1) = n^2 - n + 1 = p_i \cdot \ldots \cdot p_j$, где делители $p_i, \ldots, p_j$ тождественны 1 по *mod 6* кроме делителя, равного 3, и взяты из набора делителей порядка поля $q-1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$;

b) $X^nY^l + Y^nZ^l + X^lZ^n = 0$,

если $\Delta(n,l) = n^2 - nl + l^2 = p_i \cdot \ldots \cdot p_j$, где делители $p_i, \ldots, p_j$ тождественны 1 по *mod 6* кроме равного 3, и взяты из набора делителей порядка поля $q-1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $\gcd(n,l) = 1$;

c) $X^{cn}Y^{cl} + Y^{cn}Z^{cl} + X^{cl}Z^{cn} = 0$,

если $\Delta(cn,cl) == c^2 \cdot p_i \cdot \ldots \cdot p_j$, где делители $p_i, \ldots, p_j$ тождественны 1 по *mod 6* кроме делителя, равного 3, и все $c, p_i, \ldots, p_j$ взяты из набора делителей порядка поля $q-1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $\gcd(n,l) > 1$;

d) $X^cY^c + Y^cZ^c + X^cZ^c = 0$,

если $\Delta(c,c) = c^2$, где c есть делитель порядка поля $q-1$.

Доказательство выходит за рамки статьи и требует привлечения техники доказательств по оценкам числа точек [4]

Замечание 1.

1. Многообразие нетривиальных кривых Гурвица определяется значениями делителей порядка поля, как следует из утверждения 1.

2. Важной задачей является определение условий построения максимальных кривых Гурвица и оценка их параметров.

3. УСЛОВИЕ МАКСИМАЛЬНОСТИ КРИВЫХ ГУРВИЦА

Квадратичное поле замечательно тем, что в F_{q^2} существуют максимальные кривые, например, кривые Эрмита. Как следует из предложения 1, каждая кривая над полем F_{q^2}, которая покрывается кривой Эрмита, является F_{q^2} максимальной [3]. Основные результаты по максимальным кривым Гурвица представлены в работах F.Torres [1, 2].

Теорема 1. [1] Кривая Гурвица H_n над полем F_{q^2} является максимальной, если и только если $q+1 \equiv 0 \bmod (n^2 - n + 1)$.

Доказательство теоремы является важным, вытекает из предложения 1 и результата леммы 1. Действительно по лемме морфизм

$$(u:v:1) \to (x:y:1) = \left(u^n v^{-1} : uv^{n-1} : 1\right)$$

отображает кривую $u^{n^2-n+1} + v^{n^2-n+1} + 1 = 0$ на кривую $x^n y + y^n + x = 0$.

По условию теоремы $q+1 \equiv 0 \bmod (n^2 - n + 1)$ и кривая $u^{n^2-n+1} + v^{n^2-n+1} + 1 = 0$ принадлежит семейству кривых Эрмита. Тогда и $x^n y + y^n + x = 0$ по предложению 1 является максимальной.

Условие «только если» доказывается следующим образом. Обозначим точки кривой Гурвица на бесконечности как $P_0 := (1:0:0)$, $P_1 := (0:1:0)$ и $P_2 := (0:0:1)$. В работе Carbonne P. и др. [5] показано, что подгруппа Вейерштрасса для кривой Гурвица в точке $P_1 := (0:1:0)$ образуется набором $S := \{s(n-1)+1 : s = 1, \ldots, n\}$. Пусть λ есть линия с уравнением $X = 0$. Тогда λ пересекает кривую Гурвица χ в точках P_1 и P_2. Вычислим кратность пересечения λ с кривой χ в точке P_2 $I(P_2, \chi, \lambda)$. В точке P_2 имеем $x^n y + y^n + x = 0$ и после преобразований $x = y^n / \left(1 + x^{n-1} y\right) = 0$. Отсюда следует, что $I(P_2, \chi, \lambda) = n$. По теореме Безу кратность пересечения λ с кривой χ равна $I(\chi, \lambda) = n+1$, что определяет значение $I(P_1, \chi, \lambda) = 1$. Таким образом $\chi'' \lambda = nP_2 + P_1$. Аналогично для $\mu : Y = 0$ получим $\chi'' \mu = P_2 + nP_0$ и для $\gamma : Z = 0$ имеем $\chi \bullet \gamma = P_0 + nP_1$. Значение дивизоров рациональных функций будут равны $(x/z) = nP_2 - (n-1)P_1 - P_0$ и

$$(y/z) = (n-1)P_0 - P_2 - nP_1,$$

и

$$\left(x^{s-1} y\right) = \left(n(s-1)+1\right)P_2 + (n-s)P_0 - \left(s(n-1)+1\right)P_1.$$

Это доказывает, что набор S содержится в подгруппе Вейерштрасса $H(P_1)$ для точки P_1. Практически это означает, что $H(P_1)$ включает счетное множество чисел набора S.

Пусть кривая Гурвица является F_{q^2} максимальной. В работе [8] показано, что при характеризации Эрмитовых функциональных полей выполняется условие эквивалентности порядков рациональных функций в точках бесконечности $(q+1)P_1 \sim (q+1)P_2$. В случае $s = n$, имеем следующее представление дивизора $\left(x^{n-1} y\right) = \left(n(n-1)+1\right)P_{20} - \left(n(n-1)+1\right)P_1$. Известно, что степень дивизора рациональной функции равна 0 и имеем условие эквивалентности для порядков дивизора рациональных функций

на кривой Гурвица $\left(n^2-n+1\right)P_1 \sim \left(n^2-n+1\right)P_2$. Пусть $d=\gcd\left(n^2-n+1,q+1\right)$ и значение d в силу F_{q^2} максимальности кривой содержится в подгруппе Вейерштрасса $H(P_1)$. В соответствии с представлением Carbonne P. и др. [5] для S значение d должно иметь вид $d=A(n-1)+B$ при $A\geq B\geq 1$. Нужно показать, что $d=n^2-n+1$. Предположим, это не так и существует разложение $n^2-n+1=C\left(A(n-1)+B\right)$. После ряда преобразований имеем $BC=D(n-1)+1$ и $AD(n-1)+A+BD=Bn$ для $D\geq 0$. Левая часть последнего уравнения будет равна правой только при условии $B=C=1$ и $D=0$. Тогда $A=n$ и $d=n^2-n+1$, что завершает доказательство. ◊

Замечание 2.

1. Теорема 1 указывает на существование максимальных кривых Гурвица малого рода. Легко показать, что род кривых равен $g=\left(n^2-n-1\right)/2$ и не может быть большим, т.к. n^2-n+1 есть делитель $q+1$. Условия теоремы являются не только необходимыми, но и достаточными.

2. Эта теорема исчерпывает все максимальные кривые обычных кривых Гурвица H_n.

Условия F_{q^2} максимальности обобщенных кривых Гурвица были рассмотрены F.Torres в работах [1,2]. Основной результат представлен теоремой 2.

Теорема 2. Пусть $H_{n,l}$ есть несингулярная кривая Гурвица над полем F_{q^2}, $\gcd(n,l)=1$ и $Q=n^2-nl+l^2$ простое число. Тогда $H_{n,l}$ является максимальной, если и только если $n^2-nl+l^2\equiv 0\left\langle \mathrm{mod}\left|(q+1)\right.\right\rangle$, где $\left\langle \mathrm{mod}\left|(q+1)\right.\right\rangle$ определяет операцию по модулю делителя $q+1$.

Доказательство аналогично доказательству теоремы 1. Так как Q по условию простое, условие $n^2-nl+l^2\equiv 0\left\langle \mathrm{mod}\left|(q+1)\right.\right\rangle$ фактически определяет, что n^2-nl+l^2 является простым делителем $q+1$. Из результата леммы 2 следует морфизм кривой $u^{n^2-nl+l^2}+v^{n^2-nl+l^2}+1=0$ на кривую $x^n y^l+y^n+x^l=0$. По условию теоремы $n^2-nl+l^2\equiv 0\left\langle \mathrm{mod}\left|(q+1)\right.\right\rangle$ и кривая $u^{n^2-nl+l^2}+v^{n^2-nl+l^2}+1=0$ принадлежит семейству кривых Эрмита. Тогда и $x^n y^l+y^n+x^l=0$ по предложению 1 является максимальной.

Условие «только если» доказывается следующим образом. Пусть $P_0:=(1:0:0)$, $P_1:=(0:1:0)$ и $P_2:=(0:0:1)$ есть точки кривой Гурвица на бесконечности. Подгруппа Вейерштрасса для кривой Гурвица в точке $P_1:=(0:1:0)$ образуется набором

$$H:=\left\{\begin{matrix}(n-l)s+nt:s,y\in Z;t\geq 0,\\ -lt/n\leq s\leq (n-l)t/l\end{matrix}\right\}.$$

Пусть λ есть линия с уравнением $X=0$. Тогда λ пересекает кривую Гурвица χ в точках P_1 и P_2. Вычислим кратность пересечения λ с кривой χ в точке P_2 $I(P_2,\chi,\lambda)$. В точке P_2 имеем $x^n y^l+y^n+x^l=0$ и после преобразований $x^l=y^n/\left(1+x^{n-l}y^l\right)=0$. Так как $\gcd(n,l)=1$, следует $I(P_2,\chi,\lambda)=n$. По теореме Безу кратность пересечения λ с кривой χ равна $I(\chi,\lambda)=n+l$, что определяет значение $I(P_1,\chi,\lambda)=l$. Таким образом $\chi\bullet\lambda=nP_2+lP_1$. Аналогично для $\mu: Y=0$ получим $\chi\bullet\mu=lP_2+nP_0$ и для $\gamma: Z=0$ имеем $\chi\bullet\gamma=lP_0+nP_1$. Значение дивизоров рациональных функций будут равны

$$(x/z)=nP_2-(n-l)P_1-lP_0$$

$$\text{и } (y/z)=(n-l)P_0+lP_2-nP_1,$$

$$\text{и } \left(x^s y^l\right)=(ns+lt)P_2+\left(-ls+(n-l)t\right)P_0-$$
$$-\left((n-l)s+nt\right)P_1.$$

Так как степень дивизора рациональной функции равна 0 и $(n-l)s+nt\in H(P_1)$, что предусматривает $ns+lt\geq 0$ и $-ls+(n-l)t\geq 0$ и тогда $H\subseteq H(P_1)$.

В случае $s=n-l$ и $t=l$ имеем следующее представление дивизора $\left(x^{n-l}y^l\right)=\left(n^2-nl+l^2\right)P_2-\left(n^2-nl+l^2\right)P_1$. Имеем условие эквивалентности для порядков дивизора рациональных функций на кривой Гурвица $QP_1\sim QP_2$. Следовательно, $d=\gcd(Q,q+1)\in H(P_1)$, так как условие эквивалентности порядков рациональных функций F_{q^2} максимальных кривых определяется $(q+1)P_1\sim(q+1)P_2$. Так как $1\notin H(P_1)$ и Q простое число следует искомый результат. ◊

Рассмотрим примеры, поясняющие действие теорем 1 и 2.

Пример 1. В поле F_{q^2}, $q=2^7$ построить максимальные кривые Гурвица. По утверждению 1 п. a,b существуют нетривиальные кривые Гурвица $\mathcal{H}_{n,l}$ вида $X^nY+Y^nZ+XZ^n=0$ и $X^nY^l+Y^nZ^l+X^lZ^n=0$, если $n^2-n+1=p_i\cdot\ldots\cdot p_j$, и соответственно $n^2-nl+l^2=p_i\cdot\ldots\cdot p_j$, где делители $p_i,\ldots,p_j$ тождественны 1 по *mod 6* кроме, делителя равного 3, и взяты из набора делителей порядка поля. Имеем разложение порядка поля $q^2-1=2^{14}-1=3*43*127$ и $q+1=129=3*43$. Под условия утверждения 1 попадают делители $p_1=3$ и $p_2=43$. По теореме 1 кривая $X^nY+Y^nZ+XZ^n=0$ является максимальной, если n^2-n+1 является делителем $q+1$. Имеем три случая: $n^2-n+1=3$, $n^2-n+1=43$ и $n^2-n+1=3*43=129$. Первые два случая дают решения: $n=2$ и $n=7$. Таким образом существует тривиальная кривая $X^2Y+Y^2Z+XZ^2=0$ рода $g=1$ и числом точек $N_{2,1}=16641$ и нетривиальная $X^7Y+Y^7Z+XZ^7=0$ рода $g=21$ и числом точек $N_{7,1}=21761$. Других максимальных кривых, которые удовлетворяют условиям теоремы 1 и 2, нет.

Пример 2. В поле F_{q^2}, $q=2^9$ построить максимальные кривые Гурвица. Имеем разложение порядка поля $q^2-1=2^{18}-1=262143=3^3*7*19*73$ и $q+1=513=3^3*19$. Под условия утверждения 1 и теорем 1,2 попадают делители $p_1=3$

и $p_2 = 19$. По теореме 1 имеем три случая: $n^2 - n + 1 = 3$, $n^2 - n + 1 = 19$ и $n^2 - n + 1 = 3*19 = 57$. Первые и третий случаи дают решения: $n = 2$ и $n = 8$. Таким образом, существует тривиальная кривая $X^2Y + Y^2Z + XZ^2 = 0$ рода $g = 1$ и числом точек $N_{2,1} = 263169$ и нетривиальная $X^8Y + Y^8Z + XZ^8 = 0$ рода $g = 28$ и числом точек $N_{8,1} = 290817$. Второй случай, с делителем 19, соответствует условию теоремы 2 для $n^2 - nl + l^2 = 19$ и дает обобщенную максимальную кривую вида $X^5Y^2 + Y^5Z^2 + X^2Z^5 = 0$, рода $g = 9$ и числом точек $N_{5,2} = 271361$.

Замечание 3.

1. Теорема 1 исчерпывает все максимальные обычные кривые Гурвица H_n.

2. Теорема 2 рассматривает максимальные обобщенные кривые Гурвица $H_{n,l}$ при ограничении $\gcd(n,l) = 1$, $Q = n^2 - nl + l^2$ — простое число и $n^2 - nl + l^2 \equiv 0 \langle \bmod |(q+1)\rangle$, в то время как утверждение 4 указывает на существование четырёх разнообразий кривых Гурвица.

Следующие теоремы являются новыми и снимают ограничение на показатель $Q = n^2 - nl + l^2$.

Теорема 3. Пусть $H_{n,l}$ есть несингулярная кривая Гурвица над полем F_{q^2}, $\gcd(n,l) = 1$. Тогда $H_{n,l}$ является максимальной, если и только если $q + 1 \equiv 0 \bmod \left(n^2 - nl + l^2\right)$.

Доказательство аналогично доказательству теорем 1 и 2. Действительно, так как $n^2 - nl + l^2$ является делителем $q+1$, из результата леммы 2 следует морфизм кривой $u^{n^2-nl+l^2} + v^{n^2-nl+l^2} + 1 = 0$ на кривую $x^n y^l + y^n + x^l = 0$. Кривая $u^{n^2-nl+l^2} + v^{n^2-nl+l^2} + 1 = 0$ принадлежит семейству кривых Эрмита и $x^n y^l + y^n + x^l = 0$ по предложению 1 является максимальной.

Условие «только если» доказывается подобным образом. Имеем условие эквивалентности для порядков дивизора рациональных функций на кривой Гурвица $\left(n^2 - nl + l^2\right)P_1 \sim \left(n^2 - nl + l^2\right)P_2$. Так как условие эквивалентности порядков рациональных функций F_{q^2} максимальных кривых определяется $(q+1)P_1 \sim (q+1)P_2$, следовательно, $d = \gcd\left(n^2 - nl + l^2, q+1\right) \in H(P_1)$. Так как $1 \notin H(P_1)$ и $n^2 - nl + l^2$ есть делитель $q+1$, следует искомый результат. ◊

Теорема 3 определяет условия максимальности для обобщенных кривых п. b) из утверждения 4.

Пример 3. Рассмотрим, как в примере 3, поле F_{q^2}, $q = 2^7$. По утверждению 1 п. b) существует нетривиальная кривая Гурвица для случая $n^2 - nl + l^2 = 3*43 = 129$. Это попадает под условия максимальности теоремы 3 и дает обобщенную максимальную кривую вида $X^{13}Y^5 + Y^{13}Z^5 + X^5Z^{13} = 0$, рода $g = 64$ и числом точек $N_{13,5} = 32769$.

Следующая теорема определяет условия максимальности кривых Гурвица из п. d) утверждения 1.

Теорема 4. Пусть $H_{n,l}$ есть кривая Гурвица над полем F_{q^2}, $n = l$. Тогда $H_{n,l}$ является максимальной, если и только если $q + 1 \equiv 0 \bmod n$.

Действительно отображение морфизма $(x:y:1) \to (u:v:1) = (y:\frac{y}{x}:1)$ кривой Гурвица $x^n y^n + y^n z^n + x^n z^n = 0$ есть кривая Ферма $u^n + v^n + 1 = 0$. Если $q + 1 \equiv 0 \bmod n$ кривая $u^n + v^n + 1 = 0$ принадлежит семейству кривых Эрмита и по предложению 1 следует максимальность $x^n y^n + y^n z^n + x^n z^n = 0$. Условие «только если» доказывается, как в теореме 3. Заметим, что точки на бесконечности кривой Гурвица $P_0 := (1:0:0)$, $P_1 := (0:1:0)$ и $P_2 := (0:0:1)$ имеют кратность n. Имеем условие эквивалентности для порядков дивизора рациональных функций на кривой Гурвица $n^2 P_1 \sim n^2 P_2$. Условие эквивалентности порядков рациональных функций F_{q^2} максимальных кривых с учетом кратности точек на бесконечности определяется, как $n(q+1)P_1 \sim n(q+1)P_2$. Значение $d = \gcd\left(n^2, n(q+1)\right)$ должно содержаться в подгруппе Вейерштрасса $H(P_1)$ для точки P_1. Так как $1 \notin H(P_1)$ и n есть делитель $q+1$, следует искомый результат. ◊

Пример 4. Рассмотрим поле F_{q^2}, $q = 2^7$. По утверждению 1 п. d) существуют нетривиальные кривые Гурвица для $n = l = 3,43,127,129$. Значения $n = 3,43,129$ являются условиями максимальности по теореме 4. Например, кривая вида $X^{43}Y^{43} + Y^{43}Z^{43} + X^{43}Z^{43} = 0$ имеет род $g = 861$ и число точек $N_{43,43} = 236675$, из которых F_{q^2} рациональных 236672 и 3 точки на бесконечности с кратностью 43. Сумма точек с учетом кратности дает значение на границе Хассе-Вейля $N = 236801$.

Замечание 4. Максимальная кривая Гурвица $X^{q+1}Y^{q+1} + Y^{q+1}Z^{q+1} + X^{q+1}Z^{q+1} = 0$, тождественна кривой Эрмита $X^{q+1} + Y^{q+1} + Z^{q+1} = 0$ наибольшего рода $g = q(q-1)/2$.

Общий результат максимальности обобщенных кривых Гурвица вида c) из утверждения 1 представлен следующей теоремой.

Теорема 5. Пусть кривая Гурвица $H_{n,l}$ вида $X^{cn}Y^{cl} + Y^{cn}Z^{cl} + X^{cl}Z^{cn} = 0$, $\gcd(n,l) = 1$, $c \geq 1$ определена над полем F_{q^2}. Тогда $H_{n,l}$ является максимальной, если и только если $q + 1 \equiv 0 \bmod \left(c\left(n^2 - nl + l^2\right)\right)$.

Случаи $c = 1$ и $n = l > 1$ определяются теоремами 3 и 4. Точки на бесконечности кривой Гурвица $P_0 := (1:0:0)$, $P_1 := (0:1:0)$ и $P_2 := (0:0:1)$ имеют кратность c. Условие эквивалентности для порядков дивизора рациональных функций на кривой Гурвица имеет $c^2\left(n^2 - nl + l^2\right)P_1 \sim c^2\left(n^2 - nl + l^2\right)P_2$. Условие эквивалентности порядков рациональных функций F_{q^2} максимальных кривых с учетом кратности точек на бесконечности определяется, как $c(q+1)P_1 \sim c(q+1)P_2$. Значение $d = \gcd\left(c^2\left(n^2 - nl + l^2\right), c(q+1)\right)$ должно содержать-

ся в подгруппе Вейерштрасса $H(P_1)$ для точки P_1. Так как $1 \notin H(P_1)$ и $c\left(n^2 - nl + l^2\right)$ есть делитель $q+1$, следует искомый результат. ◊

Пример 5. Рассмотрим поле F_{q^2}, $q = 2^7$. По утверждению 1 п. c) существуют нетривиальные кривые Гурвица вида $X^{cn}Y^{cl} + Y^{cn}Z^{cl} + X^{cl}Z^{cn} = 0$, если $\Delta(cn,cl) == c^2 \cdot p_i \cdot \ldots \cdot p_j$, где делители $p_i,\ldots,p_j$ тождественны 1 по *mod 6,* кроме делителя равного 3, и все $c, p_i,\ldots,p_j$ взяты из набора делителей порядка поля $q^2 - 1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. По условию теоремы 5, если $c\left(n^2 - nl + l^2\right)$ является делителем $q+1$, кривая $H_{cn,cl}$ является максимальной. Делителями разложения $q+1$ есть числа 3,43,129. В примерах 3,5,6 построены максимальные кривые вида a,b,d) утверждения 1. По теореме 5 определим следующие максимальные кривые:

1. $X^{21}Y^3 + Y^{21}Z^3 + X^{21}Z^3 = 0$, род $g = 160$ и число точек $N_{21,3} = 65025$, с учетом кратности 3 точек на бесконечности;

2. $X^{86}Y^{43} + Y^{86}Z^{43} + X^{86}Z^{43} = 0$, род $g = 2710$ и число точек $N_{86,43} = 710145$, с учетом кратности 43 точек на бесконечности.

Теорема 5 является обобщением теорем 1-4, так как определяет условия F_{q^2} максимальности всех видов кривых Гурвица.

Важной задачей является построение наилучшей максимальной кривой Гурвица. Следующая теорема определяет максимальную кривую Гурвица наибольшего рода и соответственно с наибольшим числом точек.

Теорема 6. Пусть F_{q^2} конечное поле и $q+1 \equiv 0 \bmod 3$. Тогда обобщенная кривая Гурвица в F_{q^2} вида

$$X^{2(q+1)/3}Y^{(q+1)/3} + Y^{2(q+1)/3}Z^{(q+1)/3} + X^{(q+1)/3}Z^{2(q+1)/3} = 0 \quad (4)$$

является максимальной кривой наибольшего рода $g = g_3 = \left(q^2 - q + 4\right)/6$.

Действительно, отображение морфизма $(x:y:1) \to (u/v:v:1) = (x:y:1)$ кривой

$$x^{2(q+1)/3}y^{(q+1)/3} + y^{2(q+1)/3}z^{(q+1)/3} + x^{(q+1)/3}z^{2(q+1)/3} = 0$$

есть кривая $u^{2(q+1)/3} + u^{(q+1)/3} + v^{q+1} = 0$, которая является максимальной [1]. По предложению 1 следует максимальность кривой Гурвица. Условие «только если» доказывается, по теореме 5. Следует проверить, что $q+1 \equiv 0 \bmod \left(c\left(n^2 - nl + l^2\right)\right)$. Действительно, $c = (q+1)/3$ и $n^2 - nl + l^2 = 3$ тождество следует. Значение рода равно

$$g = \left(c^2\left(n^2 - nl + l^2\right) + 2 - (q+1)\right)/2 = \left((q+1)^2/3 + 2 - (q+1)\right)/2 = \left(q^2 - q + 4\right)/6 = g_3. \quad (5)$$

По классификации максимальных кривых это третье значение рода и наилучшая максимальная кривая Гурвица. ◊

ВЫВОДЫ

Впервые описаны семейства нетривиальных кривых Гурвица и представлены условия максимальности для кривых Гурвица общего вида со снятием ограничения на показатели степени кривой, впервые получена максимальная кривая Гурвица с третьим значением рода для максимальных кривых.

Литература.

[1] *Torres F.* Plan maximal curves, Acta Arith. 98(2) (2001), 165-179.

[2] *Cossidente A., Korchm'aros G. and Torres F.,* Curves of large genus covered by the Hermitian curve. Comm. Algebra 28(10), 4707–4728 (2000).

[3] *Carbonne P., Henocq T.,* Decomposition de la Jacobienne sur les corps finis. Bull. Polish Acad. Sci. Math. 42(3) (1994), 207-215.

[4] *Халимов Г.З.* Оценка параметров кривых Гурвица для целей универсального хеширования. Сб. трудов Первой международной научно-технической конференции "Компьютерные науки и технологии". Белгород, Россия. 8-10 октября 2009 г., ч. 2, с 118-121.

[5] *Jurgen Bierbrauer.* Authentication via algebraic-geometric codes. URL http://www.math.mtu.edu/~jbierbra/potpap.ps.

[6] *Халимов Г.З.* Максимальные кривые Гурвица для целей универсального хеширования. Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 3. – Таганрог: Изд-во ТТИ ЮФУ, 2010. с.144-146

[7] *Lachaud G.* Sommes d'Eisenstein et nombre de points de certaines courbes algebriques sur les corps finis, C.R. Acad.Sci. Paris 305,Serie 1 (1987), 729-732.

[8] *Ruck H.G. and Stichtenoth,* A characterization of Hermition function fields over finite, J. Reine Angew. Math. 457, 185-188 (1994).

Поступила в редколлегию 2.06.2010.

Халимов Геннадий Зайдулович, канд. техн. наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: методы и средства высокоскоростной аутентификации данных.

УДК 681.3.06

Універсальне хешування за максимальними кривими Гурвіца / Г.З. Халімов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 365-369.

Представлені результати досліджень по максимальних кривих Гурвіця для цілей універсального хешування, умови максимальності узагальнених кривих, максимальна крива Гурвіця з третім значенням роду.

Ключові слова: універсальне хешування, криві Гурвіця.

Бібліогр.: 08 найм.

UDC 681.3.06

Universal hashing by the maximum of Hurwitz curves / G.Z. Halimov// Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 365-369.

The results of studies on the maximum Hurwitz curves for universal hashing and conditions for maximum generalized curves, the maximum Hurwitz curves with the third genus value are provided.

Key words: universal hashing, Hurwitz curves.

Ref.: 08 items.

УДК 519:616-079.4:616.5

ПАРАЛЛЕЛЬНЫЕ ВЫЧИСЛЕНИЯ В КРИПТОГРАФИЧЕСКИХ АЛГОРИТМАХ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Е.Г. КАЧКО, С.С. БАТЮШКО

В статье рассмотрены параллельные варианты вычислений для полиномов, точек эллиптической кривой и скалярного произведения с целью уменьшения их вычислительной сложности. Использование предложенных алгоритмов позволило существенно увеличить эффективность вычислений.

Ключевые слова: криптография, цифровая подпись, эллиптические кривые, параллельные вычисления

1. ПОСТАНОВКА ЗАДАЧИ И ЕЕ АКТУАЛЬНОСТЬ

Большинство современных несимметричных криптографических алгоритмов используют операции над эллиптическими кривыми. Это связано с тем, что эллиптические кривые позволяют уменьшить размер цифровой подписи без уменьшения криптографической стойкости алгоритмов. Примерами таких алгоритмов являются стандарты [1–3]. С другой стороны, большинство современных процессоров являются много ядерными. Поэтому актуальной является задача разработки параллельных алгоритмов как для простых операций над полями, так и основной операции, лежащей в основе формирования и проверки цифровой подписи – скалярного умножения точки эллиптической кривой на скаляр.

В данной работе рассматривается преобразование последовательных алгоритмов в параллельные для выполнения операций над целыми числами, полиномами и точками эллиптической кривой. Для каждого типа алгоритма определяются теоретические оценки с учетом числа ядер процессора и параметров эллиптической кривой. Приведены практические результаты, получаемые за счет их параллельного выполнения, для 2-х ядерного процессора.

2. МОДУЛЬНОЕ ВОЗВЕДЕНИЕ В СТЕПЕНЬ

Операция модульного возведения в степень используется для проверки простоты числа [1–3]. Эта проверка выполняется для формирования параметров эллиптической кривой для всех типов алгоритмов. Для операции используется, как правило, блочный алгоритм Кнута, реализация которого описана в [4]. Суть алгоритма состоит в последовательном выполнении операций вычисления квадрата и умножения с многократной точностью. Для параллельного вычисления степени можно разделить показатель степени на порции и вычислять степень для каждой порции параллельно. Число порций совпадает с числом ядер процессора, а размер порции определяется с учетом того, что после вычисления степени ее необходимо откорректировать с учетом позиции порции. Ускорение [5] за счет параллельных вычислений определяется как отношение времени наилучшего последовательного и параллельного алгоритмов.

Приведенный алгоритм позволил получить ускорение от 20 до 50% в зависимости от числа ядер. В табл. 1 приведены результаты экспериментальной проверки алгоритма для двух ядерного процессора.

Таблица 1

Временные характеристики последовательного и параллельного вычисления модульного возведения в степень[1]

Модуль преобразования	Время (с) при последовательном выполнении	Время (с) при параллельном выполнении (2 ядра)	Ускорение
1024	0.0466112	0.0387393	1.2032
2048	0.349978	0.2901	1.20641
3072	1.15529	0.949829	1.21631

3. ПОЛИНОМИАЛЬНЫЕ ОПЕРАЦИИ

Стандарт [1] наряду с простым полем использует двоичное поле $GF(2^m)$, стандарт [3] полностью построен на использовании двоичного поля $GF(2^m)$. В этом случае вместо традиционных арифметических операций над числами многократной точности используются операции над полиномами. Все полиномиальные операции выполняются с учетом модуля (неприводимого полинома). Основная идея параллельного выполнения состоит в том, что вычисление значения и вычисление модуля выполняется параллельно. Удалось полностью совместить операции вычисления квадрата полинома, операции умножения и инверсии удалось параллельно выполнить лишь частично. Эффективность параллельных вычислений для операций этого класса будет рассмотрена ниже.

4. СКАЛЯРНОЕ УМНОЖЕНИЕ

Операция скалярного умножения выполняется и на этапе формирования, и на этапе проверки цифровой подписи. Для параллельного выполнения операции скалярного умножения на этапе формирования цифровой подписи используются те же идеи, что и при вычислении модульной операции возведения в степень, рассмотренные выше. Особенностью операции проверки цифровой подписи является необходимость вычисления

[1] Все эксперименты выполнены на вычислительной системе с процессором Intel(R) Pentium (R) Dual CPU E2160 @ 1.80 GHz в среде Visual Studio 2005, с поддержкой Open MP.

двух скалярных умножений, причем для второй операции предвычисления не могут быть выполнены, так как используется каждый раз новый открытый ключ. Вот почему операция проверки цифровой подписи обычно выполняется значительно дольше, чем операция ее формирования. Это приводит к дисбалансу системы, использующей цифровые подписи. Вот почему проблема сближения времени формирования и проверки цифровой подписи является столь же важной, как и проблема ускорения самих операций.

В работе предложены алгоритмы параллельного выполнения указанных выше операций и исследовано соотношение между временами формирования и проверки цифровой подписи.

Параллельное вычисление основано на делении скаляра на порции и обработке каждой порции параллельно. Для определения размеров порций определялось соотношение времен операций удвоения (D) и сложения (A) точек. В табл. 2 приведены экспериментальные результаты для полиномиального базиса ДСТУ 4145-2002 значений D, A, число итераций d для Comb метода, а также экспериментальное значение ускорения (S).

Таблица 2

Отношение времен операций удвоения и сложения точек (для якобиановский координат), размер окна равен 8

№	m	D (мкс.)	A (мкс.)	R = = A / D	Число циклов (d)	S
1	163	9.23485	37.5794	4.0693	20	1,70
2	167	8.10486	22.8046	2.8137	20	1,70
3	173	9.63484	23.7146	2.46134	21	1,70
4	179	8.51486	23.5096	2.76101	22	1,71
5	191	8.09486	22.9396	2.83385	23	1,71
6	233	11.0098	30.8745	2.80427	29	1,72
7	257	11.6498	33.5744	2.88197	31	1,72
8	307	14.8898	39.0193	2.62055	38	1,72
9	367	16.6897	47.8992	2.86998	45	1,73
10	431	22.1446	60.4090	2.72793	53	1,73

Для последовательных вычислений в общем виде необходимо d операций удвоения и сложения, т.е. время вычислений равно $d (D + A) = d D (1 + r) = 4 d D$.

Параллельные вычисления

Рассмотрим определение размера порции для двух ядерного процессора. Пусть старшая часть задается k цифрами, тогда младшая часть d – k цифр.

Для вычисления старшей части необходимо выполнить d операций удвоения и k операций сложения. Т.е. время вычисления равно

$$k (D + A) + (d – k) D.$$

Для вычисления младшей части необходимо выполнить (d – k– 1) операций удвоения и сложения. Время вычисления младшей части составляет (d – k – 1) (D + A).

Для достижения максимального эффекта обе части должны завершиться одновременно. Определим значение k для этого.

$$(d – k –1) (D + A) = k (D + A) + (d – k) D.$$

Так как r = A / D, то k = (dr – 1 - r) / (1 + 2r).

После округления в большую сторону получаем k = (dr – 1 + r) / (1 + 2r).

Из табл. 2 следует, что r ≈ 3, т.е. k = (3d +2)/7.

Так, для m = 163 число итераций для обработки старшей части равно 8 и число итераций для младшей части равно 12.

Время выполнения операций для параллельного вычисления равно:

$$k (D + A) + (d- k) * D + A = (16dD + 9D)/7.$$

Теоретическое ускорение для параллельных вычислений:

$$S = 4 d D * 7 / (16dD + 9D) = 28d/(16d + 9) \approx 7/4.$$

Из последней формулы видно, что ускорение тем больше, чем больше d. Величина ускорения не превышает 1,75, т.е. 75 процентов для двух ядер. Значения ускорений, полученные в результате вычислительного эксперимента, приведены в табл. 2 (последняя колонка).

Реальное ускорение меньше расчетного за счет того, что после вычисления скалярного произведения в полярных координатах результат необходимо перевести в аффинные координаты. Кроме этого, теоретические расчеты не учитывают накладных расходов, связанных с формированием потоков.

Для проверки цифровой подписи необходимо выполнить 2 операции скалярного умножения. Если процессор содержит 4 или более ядер, то каждую операцию можно выполнять параллельно. Если используется двух ядерный процессор, то одна итерация должна соответствовать одной операции скалярного умножения.

В табл. 3, 4 приведены результаты экспериментального исследования предложенных алгоритмов на примере ДСТУ 4145-2002, которые достигаются за счет параллельного выполнения базовых операций для работы с полиномом, точками эллиптической кривой и вычисления скалярных умножений.

Таблица 3

Формирование (S)и проверка (V)цифровой подписи для последовательного режима выполнения

№	m	Последовательный (Ts)		
		S	V	V/S
1	163	0,783699	2,42131	3,09
2	167	0,763359	2,40964	3,16
3	173	0,808407	2,46914	3,05
4	179	0,854701	2,6455	3,10
5	191	0,878735	2,76625	3,15
6	233	1,35044	4,41501	3,27
7	257	1,59109	5,44959	3,43
8	307	2,17865	7,38007	3,39
9	367	3,09598	10,989	3,55
10	431	4,31034	15,625	3,63
11	571	7,8125	28,5714	3,66

Обозначения в таблице: m – степень поля; S – время формирования цифровой подписи (миллисекунд); V – время проверки цифровой подписи (миллисекунд); S/V – отношение времени проверки к времени формирования цифровой подписи.

Таблица 4

Формирование (S) и проверка (V) цифровой подписи для параллельного режима выполнения

№	M	Параллельный (Tp)			Ускорение (Ts/Tp)	
		S	V	V/S	S	V
1	163	0,558347	0,855798	1,53	1,40	2,83
2	167	0,547945	0,838574	1,53	1,39	2,87
3	173	0,594354	0,903751	1,52	1,36	2,73
4	179	0,61237	0,921234	1,50	1,40	2,87
5	191	0,637349	0,990099	1,55	1,38	2,79
6	233	0,967586	1,52207	1,57	1,40	2,90
7	257	1,12423	1,77936	1,58	1,42	3,06
8	307	1,5361	2,11416	1,38	1,42	3,49
9	367	2,11416	3,68324	1,74	1,46	2,98
10	431	2,99401	5,27704	1,76	1,44	2,96
11	571	5,49451	9,70874	1,77	1,42	2,94

В последних двух колонках табл. 4 приведены значения ускорений для формирования (S) и проверки (V) цифровой подписи.

На рис. 1 изображены графики зависимости отношения времен для проверки и генерации цифровой подписи.

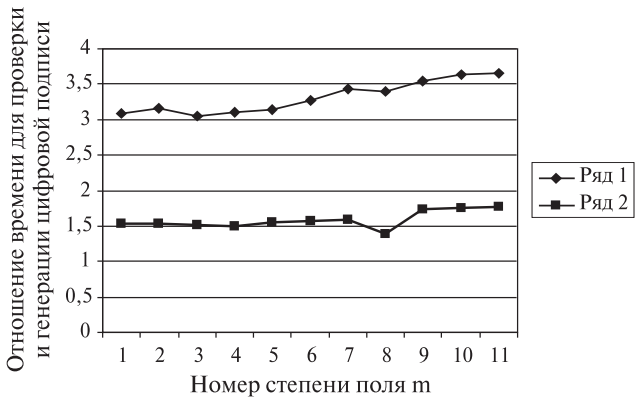


Рис. 1. Отношение времени для проверки и генерации цифровой подписи для последовательного и параллельного алгоритмов:
ряд 1 – последовательный алгоритм;
ряд 2 – параллельный алгоритм

Как видно из рисунка, соотношение времен незначительно зависит от степени поля m. Если проигнорировать выброс значения отношения для номера степени 8 (m = 307), то из графика для параллельных вычислений следует, что это значение плавно увеличивается в пределах 8%, такой же приблизительно относительный прирост отношения этих времен для последовательных вычислений.

Таким образом, характер изменений степени эллиптической кривой на изменение отношения времени для проверки и формирования цифровой подписи не зависит от выбора типа вычислений.

ВЫВОДЫ

Параллельное выполнение базовых операций для эллиптических кривых позволило получить следующие результаты:

– среднее значение ускорения для формирования цифровой подписи составляет 1.41 и для ее проверки — 2.95;

– ускорение практически не зависит от значения *m* поля Галуа эллиптической кривой (отклонение от математического ожидания не превосходит 3.5 % для цифровой подписи и 18 % для проверки цифровой подписи);

– параллельное выполнение проверки подписи более эффективно, чем формирования подписи, так как при проверке подписи соотношение между параллельно и последовательно выполняемым кодом выше (Закон Амдаля);

– использование параллельных вычислений позволяет существенно улучшить соотношение между временем формирования и проверки цифровой подписи. В случае последовательных вычислений это значение не менее 3,09 и растет с увеличением m, в случае параллельных вычислений максимальное значение отношения равно 1.77.

Литература.

[1] FIPS PUB 186-3. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Digital Signature Standard (DSS) Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900 Issued June, 2009.

[2] ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [http://dic.academic.ru/dic.nsf/ruwiki/261586].

[3] ДСТУ 4145-2002. Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ, Держстандарт України. 2003. 36 с.

[4] *Качко Е.Г., Свинарев А.В., Головашич С.А., Лавриненко Д.И.* «Исследование методов оптимизации криптографических операций» Материалы юбилейной научно-технической конференции “Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”, Киев, 1998, 198-203.

[5] *Воеводин В.В., Воеводин Вл.В.* Параллельные вычисления. СПб: БХВ – Петербург, 2004. – 608 с.

Поступила в редколлегию 4.06.2010.

Качко Елена Григорьевна, кандидат технических наук, профессор кафедры ПОЭВМ ХНУРЭ. Область научных интересов: программные средства криптографических систем.

Батюшко Стас Стефанович, ассистент кафедры БИТ ХНУРЭ. Область научных интересов: защита информации в телекоммуникационных сетях, операционные системы, языки программирования, отказостойкие системы, создание больших разветвленных вычислительных систем, суперкомпьютеры.

УДК 519:616-079.4:616.5

Паралельні обчислення в критографічних алгоритмах на основі еліптичних кривих / Е.Г. Качко, С.С. Батюшко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 370-373.

В статті розглядаються паралельні варіанти обчислень для поліномів, точок еліптичної кривої та скалярного додатку з метою зменшення обчислювальної складності операцій формування та перевірки цифрового підпису. Використання запропонованих алгоритмів дозволило суттєво збільшити ефективність обчислень.

Ключові слова: криптографія, цифровий підпис, еліптичні криві, паралельне обчислення.

Табл. 04. Іл.01. Бібліогр.: 05 найм.

UDC 519:616-079.4:616.5

Parallel calculations in elliptic curve cryptographic algorithms / E.G. Kachko, S.S. Batyushko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 370-373.

The paper considers parallel variants of calculations for polynomials, elliptic curve points and scalar product with the aim of diminishing their computational complexity. The use of the algorithms suggested allowed to substantially increase the efficiency of calculations.

Key words: cryptography, digital signature, elliptic curves, parallel calculations.

Tab. 04. Fig. 01. Ref.: 05 items.

УДК 681.3.06

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ВАРИАНТОВ ПРЕДСТАВЛЕНИЙ БОЛЬШИХ ЧИСЕЛ ПО МНОЖЕСТВЕННЫМ ОСНОВАНИЯМ В НЕСИММЕТРИЧНОЙ КРИПТОГРАФИИ

О.А. МЕЛЬНИКОВА, А.С. БУТЕНКО

В статье приведены результаты исследования эффективности методов выполнения скалярного умножения с использованием представлений больших чисел по множественным основам. В работе предлагаются результаты сравнительного анализа реализаций методов между собой и с реализацией метода, что использует знаково-цифровые представления чисел. На основе приведенных результатов сделаны выводы относительно эффективности методов выполнения скалярного умножения с использованием представлений больших чисел по множественным основам и рассмотрены перспективы последующих исследований.

Ключевые слова: несимметричная криптография, скалярное умножение.

ВВЕДЕНИЕ

Криптосистемы на основе эллиптических кривых обеспечивают требуемый уровень безопасности при меньших размерах ключа и, вследствие этого, имеют явные преимущества над другими асимметричными методами. При практическом внедрении криптосистем на основе эллиптических кривых особую актуальность приобретают вопросы эффективной реализации основных операций. Большинство криптографических протоколов на эллиптических кривых требует вычисление скалярного произведения. Таким образом, требуется разработать быстрые алгоритмы вычисления скалярного произведения $[k]P$ для любого целого числа k и для любой точки P эллиптической кривой.

В статье представлены результаты исследования эффективности скалярного умножения на основе методов представления больших чисел по множественным основаниям: представление чисел по двойным основаниям с нетривиальными коэффициентами (Extended DBNS [1]), представление чисел по двойным основаниям с построением бинарного дерева (Tree-based DBNS [2]) и представление чисел по тройным основаниям с нетривиальными коэффициентами (SMBR [3]).

В данной статье рассматриваются эллиптические кривые над расширенным двоичным полем $E(GF(2^m))$. Как известно, наиболее вычислительно сложной операцией является инверсия элемента поля [3]. Для того, чтобы исключить эту операцию, берём за основу проективные координаты. На сегодняшний день известно несколько их типов. Наиболее эффективными проективными координатами для выполнения групповых операций для $E(GF(2^m))$ являются координаты Лопеса-Дахаба [4].

В этой статье представлены результаты, полученные в ходе экспериментального сравнения реализаций указанных методов, а также сравнения с функцией скалярного умножения ecurve2_mult из библиотеки MIRACL [5], в которой используются знаково-цифровые представления чисел. Необходимо отметить, что ранее уже проводилось сравнение реализации скалярного умножения на основе метода представления больших чисел по множественным основаниям, использующего “золотое сечение”, с функцией скалярного умножения ecurve2_mult. Метод с использованием “золотого сечения” дал уменьшение вычислительной сложности скалярного умножения по сравнению с функцией скалярного умножения ecurve2_mult для аффинных координат.

1. КЛАССИФИКАЦИЯ МЕТОДОВ

Представлением числа k по множественным основаниям называется представление в виде суммы степеней элементов набора “маленьких” целых чисел $B=\{b_1,...,b_j\}$:

$$k=\sum_{i=1}^{m} s_i b_1^{e_{ij}} ... b_j^{e_{ij}}, \qquad (1)$$

где $|s_i|\in S$, $|b_j|\in B$.

Система представлений по двойным основаниям (DBNS) является частным случаем представления по множественным основаниям с количеством оснований $\#B=2$. В данной работе рассматривается вариант с набором оснований $B=\{2,3\}$. В системе представления по двойным основаниям любое целое число k может быть представлено в виде:

$$k=\sum_{i=1}^{m} s_i 2^{a_i} 3^{b_i}, \qquad (2)$$

где $|s_i|\in S$.

Метод Extended DBNS использует ограничения (3) на значения a_i, b_i и наборы коэффициентов $S=\{1,5,7,11,13,17,19,23,25...\}$, состоящие из чисел, взаимно простых с 2 и 3. Необходимо отметить, что авторами данной работы были проведены эксперименты с использованием других наборов коэффициентов. Однако при использовании указанного набора коэффициентов была получена самая высокая эффективность поиска представлений чисел:

$$a_1 \ge a_2 \ge ... \ge a_m \qquad (3)$$
$$b_1 \ge b_2 \ge ... \ge b_m .$$

Метод Tree-based DBNS основан на построении бинарных деревьев. Данный подход не ограничивается нахождением одного разложения числа (2). В Tree-based DBNS выполняется заданное количество разложений, равное границе T, и выбирается лучшее среди них.

Система представлений по тройным основаниям является частным случаем представления по множественным основаниям с количеством оснований $\#B = 3$. В данной работе рассматривается вариант с набором оснований $B = \{2,3,5\}$. В системе представления по тройным основаниям любое положительное число k может быть представлено в виде:

$$k = \sum_{i=1}^{m} s_i 2^{a_i} 3^{b_i} 5^{c_i}, \quad (4)$$

где $|s_i| \in S$.

Метод SMBR использует ограничения (5) на значения a_i, b_i, c_i и наборы коэффициентов $S = \{1,7,11,13,17,19,23,29,31...\}$, состоящие из чисел, взаимно простых с 2, 3 и 5.

$$\begin{aligned} a_1 &\geq a_2 \geq ... \geq a_m \\ b_1 &\geq b_2 \geq ... \geq b_m \\ c_1 &\geq c_2 \geq ... \geq c_m \end{aligned} \quad (5)$$

2. АНАЛИЗ ПРЕДСТАВЛЕНИЙ ПО МНОЖЕСТВЕННЫМ ОСНОВАНИЯМ

При исследовании скалярного умножения на основе представлений по множественным основаниям эксперименты проводились на выборках по 1000 скалярных множителей для каждой из 13 тестовых эллиптических кривых стандартов [6, 7].

Анализируемые методы требуют использования предвычислений. При этом размер таблицы предвычислений определяется значениями границ P (максимальная степень основания 3) и Q (максимальная степень основания 5, только для SMBR), а также количеством коэффициентов $\#S$. Для метода Tree-based DBNS изменяется размер бинарного дерева (граница T).

В табл. 1 приведены параметры из [1-3], использованные при исследовании указанных методов.

Таблица 1

Значения параметров

Метод	P	Q	T	$\#S$
Extended DBNS	5 – 200	—	—	1 – 13
Tree-based DBNS	5 – 200	—	1 – 16	1
SMBR	85 – 200	40 – 70	—	5 – 13

Был проведен анализ и поиск оптимальных значений параметров реализаций указанных методов, которые приведены в табл. 2.

Таблица 2

Оптимальные значения параметров

Метод	P	Q	T	$\#S$
Extended DBNS	5	–	–	9
Tree-based DBNS	5	–	4 – 8	1
SMBR	85 – 100	40 – 70	–	9

На рис. 1 представлены оценки эффективности поиска разложений больших чисел по рассмотренным методам. Количество термов метода SMBR ниже на 40-55% и 50-65% по сравнению с методами Extended DBNS и Tree-based DBNS соответственно.

На рис. 2 приведены сравнительные оценки вычислительной сложности (времени выполнения) реализаций скалярного умножения рассмотренных методов (без учёта этапа разложения), а также функции скалярного умножения ecurve2_mult. Вычислительная сложность скалярного умножения по методу Extended DBNS ниже на 20-25% и 25-40% по сравнению с методами SMBR и Tree-based DBNS соответственно. Из реализаций рассмотренных методов только Extended DBNS дал уменьшение вычислительной сложности скалярного умножения до 12% по сравнению с функцией скалярного умножения ecurve2_mult.

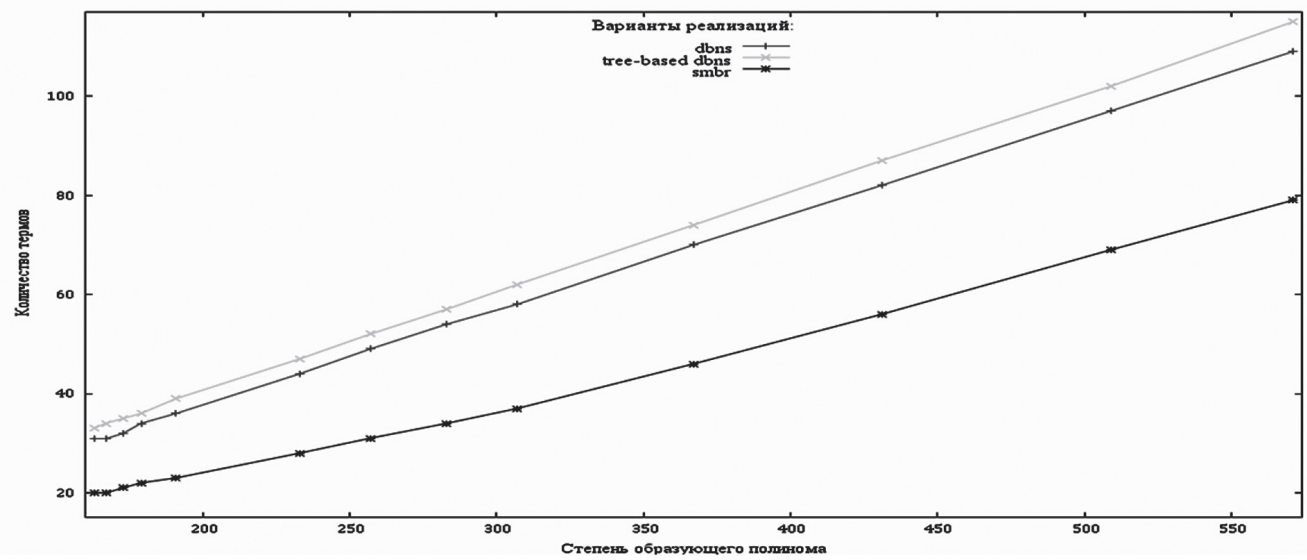


Рис. 1. Сравнение длин разложений

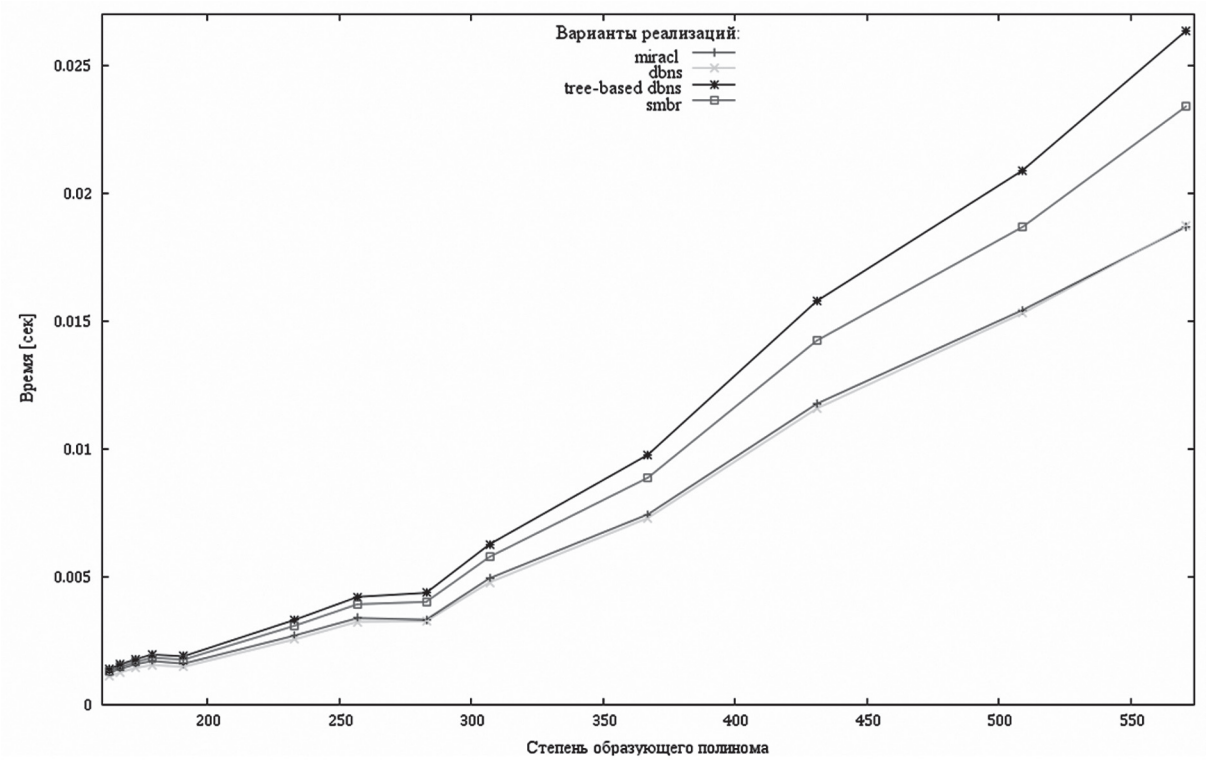


Рис. 2. Сравнение времени скалярного умножения

ЗАКЛЮЧЕНИЕ

Анализ полученных результатов показал, что для уменьшения вычислительной сложности реализаций скалярного умножения рассмотренных методов по сравнению с функцией скалярного умножения ecurve2_mult необходимо существенно уменьшить вычислительную сложность как этапа поиска разложений чисел, так и скалярного умножения чисел.

Для снижения вычислительной сложности этапа поиска разложений чисел необходимо уменьшить время поиска разложений чисел. Авторами данной работы была уменьшена вычислительная сложность преобразования больших чисел в бинарные строки, которые необходимы для нахождения разложений, что привело к уменьшению вычислительной сложности поиска представлений чисел на 100-105%. Однако вычислительная сложность преобразования больших чисел в бинарные строки составляет более 60% вычислительной сложности этапа поиска разложений чисел. В дальнейшем необходимо рассмотреть альтернативные алгоритмы поиска разложений больших чисел по множественным основаниям без использования преобразования чисел в бинарные строки.

Однако при уменьшении времени поиска необходимо не снизить эффективность поиска (длины разложений), которая влияет на вычислительную сложность этапа скалярного умножения. Также для снижения вычислительной сложности этапа скалярного умножения чисел необходимо оптимизировать операции утроения (1.2, 1.4) и упятерения (1.4) для проективных координат Лопеса-Дахаба либо другого более эффективного типа координат. Как известно из литературы [8], существуют оптимизированные формулы утроения в проективных координатах Лопеса-Дахаба, которые на момент написания статьи отсутствуют в открытом доступе.

Литература

[1] *C. Doche and L. Imbert,* “Extended double-base number system with applications to elliptic curve cryptography” // Progress in Cryptology, INDOCRYPT’06, ser. Lecture Notes in Computer Science, vol. 4329. Springer, 2006, pp. 335–348.

[2] *Doche, C., Habsieger, L.:* “A Tree-Base Approach for Computing Double-Base Chains” // ACISP 2008, ser. Lecture Notes in Computer Science, vol. 5107, pp. 433-446.Springer, Heidelberg (2008).

[3] *Dimitrov, V., Mishra, P.K.:* “Efficient Quintuple Formulas for Elliptic Curves and Efficient Scalar Multiplication using Multibase Number Representation” // ISC 2007, ser. Lecture Notes in Computer Science, vol. 4779, pp. 390-406. Springer, Heidelberg (2007).

[4] *T. Lange:* “A notes on Lopez-Dahab coordinates” // Cryptology ePrint Archive, report 2002/323, 2002.

[5] Shamus Software Ltd: “M.I.R.A.C.L Users Manual”// 4 Foster Place North, Ballybough, Dublin 3, Ireland, 2010.

[6] ДСТУ 4145 – 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – Перше видання; Введ. 1.07.2003. — К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003 р. — 36 с.

[7] Federal Information Processing Standards Publication 186 – 2 (FIPS PUB 186 - 2). Digital Signature Standard // U.S. Department of Commerce. Technology Administration, National Institute of Standards and Technology (NIST). – 2001. – 74 pp.

[8] *Haihua Gu, Dawu Gu, Ya Liu:* "Efficient Scalar Multiplication for Elliptic Curve over Binary Field"// ChinaCrypt'2008, Wuhan, Oct.2008.

Поступила в редколлегию 7.06.2010.

Мельникова Оксана Анатольевна, кандидат технических наук, доцент кафедры БИТ ХНУРЕ. Область научных интересов: защита информации, криптография.

Бутенко Александр Сергеевич, магистр кафедры БИТ ХНУРЭ. Область научных интересов: оптимизация и криптоанализ.

УДК 681.3.06

Дослідження ефективності варіантів подань великих чисел по множинним основам у несиметричній криптографії / О.А. Мельникова, О.С. Бутенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 374-377.

У статті приведені результати дослідження ефективності методів виконання скалярного множення з використанням подань великих чисел по множинним основам. У роботі пропонуються результати порівняльного аналізу реалізацій методів між собою та з реалізацією метода, що використовує знаково-цифрові подання чисел. На основі приведених результатів зроблені висновки стосовно ефективності методів виконання скалярного множення з використанням подань великих чисел по множинним основам та розглянуті перспективи подальших досліджень.

Ключові слова: несиметрична криптографія, скалярне множення.

Іл. 2. Табл. 2. Бібліогр.: 8 найм.

UDK 681.3.06

Researching effectiveness of multibase big number representation methods for using in public key cryptography / O.A. Melnikova, O.S. Butenko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 374-377.

This paper presents efficiency estimations of scalar multiplication methods which use multiple base big number representations. Comparative analysis results of methods implementations are proposed. Comparison is made not only between the methods under consideration, but also with the signed-digit representation method implementation. Conclusions about efficiency of different scalar multiplication methods are made. Possibilities of further improvements are analyzed.

Key words: public key cryptography, scalar multiplication.

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

УДК 004.056.52:004.057.4

МЕХАНІЗМИ ТА ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ ЕЛЕКТРОННОГО ПАСПОРТУ ОСОБИ

Ю.І. ГОРБЕНКО, Д.В. ПОВТАРЄВ, О.С. ТОЦЬКИЙ

Наводяться результати аналізу проблемних питань автентифікації електронного паспорта, розглядаються можливі механізми автентифікації . Основною метою аналізу є обґрунтування вимог та визначення умов застосування електронних цифрових паспортів в Україні. До основних задач відноситься проведення комплексного аналізу механізмів та внесення рекомендацій щодо усунення недоліків та загроза безпеці інформації.

Ключові слова: електронний паспорт, автентифікація, базовий контроль доступу.

ВСТУП

На даному етапі свого розвитку Україна, вслід за більшістю розвинених держав світу, планує впровадити в обіг електронний цифровий закордонний паспорт громадянина України. Ця задача потребує використання провідних технологій, що існують в наш час у світі. Разом з цим необхідно також звертати увагу і на деякі недоліки та помилки, що їх було виявлено країнами, які вже перейшли на біометричні паспорти та вживати необхідних заходів заради того, щоб надійність українського паспорту була беззаперечною. Зважаючи на такі потреби держави, існує нагальна необхідність проведення глибокого аналізу методів, механізмів та протоколів, що визначені у стандартах ІСАО[1-3].

Нині Україна повинна вирішувати різноманітні проблеми європейської інтеграції. Але по суті країна, на території якої знаходиться географічний центр континенту, фактично позбавлена можливості мати щільний контакт з членами об'єднаної Європи. Це в першу чергу пов'язано із заходами з попередження терористичної загрози, нелегальної імміграції та іншими викликами сучасності. Суровий контроль в посольствах та консульствах, важка процедура отримання віз, тривала процедура проходженням митного контролю забирають багато часу й сил, суттєво обмежують можливості перетину кордону для великої групи громадян України. Одним із засобів, що покликаний допомогти у вирішенні проблеми інтеграції, є впровадження електронного паспорту – інструменту, що допоможе підвищити рівень безпеки, довіри до документів і в той же час забезпечити простоту його використання власниками. Основною відмінністю електронних документів від існуючих паперових аналогів є те, що в них може бути внесений біометричний набір даних, такий як відбитки пальців і райдужна оболонка ока, замінити які важче ніж надрукований набір даних, і відповідно набагато важче видавати себе за власника паспорта. Біометричні дані є особливо критичною інформацією, доступ до якої мають отримувати виключно ті системи перевірки, які можуть підтвердити свої повноваження на дані дії. Для забезпечення захищеності особистої інформації власника паспорта в сучасних електронних паспортах застосовується комплекс механізмів, спрямованих на запобігання різноманітних особливо небезпечних загроз. Аналіз цих механізмів та визначення вимог до них і є основною задачею цієї роботи.

1. ОПИС СУТНОСТІ ТА ТЕХНОЛОГІЇ ЗАСТОСУВАННЯ БІОМЕТРИЧНОГО ПАСПОРТУ

Біометричний паспорт – це документ, що дає право на виїзд за межі країни і в'їзд до іноземних країн. Біометричний закордонний паспорт відрізняється від звичайного тим, що в нього вбудовано спеціальний чип, який містить двовимірну фотографію його власника, а також його дані: прізвище, ім'я, по батькові, дату народження, номер паспорта, дату його видачі і закінчення терміну дії [4, 5]. Всі електронні паспорти містять наступний символ (рис. 1):

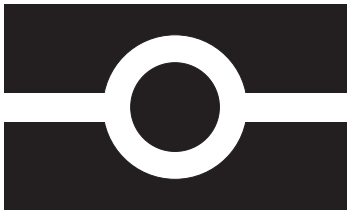


Рис. 1. Символ біометричного паспорту

Термін дії електронного паспорта встановлюється на розсуд держави видачі; однак, беручи до уваги обмежену зносостійкість документів і зміни з часом зовнішнього вигляду власника паспорта, рекомендується, щоб термін дії становив не більше десяти років. Держави можуть розглянути питання про встановлення більш короткого терміну, наприклад з метою поступової модернізації електронного паспорта в міру розвитку технології.

У багатьох європейських країнах і в США на прикордонних пунктах встановлено обладнання, яке дозволяє зчитувати дані з мікрочипу [5]. Власники біометричних закордонних паспортів користуються спеціальними коридорами, тому що внесення інформації з електронних паспортів в прикордонні системи контролю відбувається

практично миттєво, на відміну від внесення інформації з паперового носія.

США і Європа визначили біометричну ідентифікацію тих хто перетинає їхні кордони як стратегічний напрям на найближчі роки. Таким чином, найближчим часом відсутність чи наявність біометричного закордонного паспорта може стати ще одним критерієм, що буде визначати дозвіл або відмову на відвідування цих країн.

Основними джерелами з питань біометричного паспорту є різноманітні публікації організації цивільної авіації ICAO. Це, в першу чергу, Doc 9303, що складається з кількох частин. Основоположною є частина 1 «Машинозчитуємі паспорти» том 2 «Специфікації на електронні паспорти з засобами біометричної ідентифікації». Окрім основного документа Doc 9303, до нормативноправової бази ICAO входять інші міжнародні документи. Так, для досягнення одного з ключових факторів системи електронних цифрових паспортів, а саме глобальної інтероперабельності, усі розробки щодо паспортної системи повинні підпорядковуватися певному переліку стандартів ISO та ICAO.

ICAO має постійно діючу технічно консультативну групу з машинозчитувальних проїзних документів (TAG / M RTD) та робочу групу з новітніх технологій (NTWG), які регулярно представляють результати своєї роботи на конференціях ICAO та публікують їх в загальнодоступних джерелах.

Крім того, Федеральне відомство з питань інформаційної безпеки Німеччини (Bundesamt für Sicherheit in der Informationstechnik) займає активну позицію в питанні впровадження новітніх технологій як в паспортній системі Німеччини, так і на світовій арені. Конкретні шляхи вирішення питань в сфері електронних паспортів та передові дослідження публікуються співробітниками на сайті чи в збірках робот різноманітних міжнародних конференцій.

В Україні прийнято та діють нормативно – правові акти, що повинні бути використаними при входженні України в міжнародну електронну паспортну систему, проте їх обсяг та якість поки що не є достатньою, крім того, вони повинні бути узгоджені з міжнародними вимогами, особливо в частині безпеки інформації.

Аналіз вимог ICAO щодо використання електронних паспортів з біометричними даними про власника показав, що для найбільш високого рівня захисту необхідне використання комплексу механізмів, спрямованих на запобігання різноманітним загрозам.

Серед особливо небезпечних загроз необхідно виділити такі:

– компрометація змісту об'єкту захисту документу і логічної структури даних;

– точне копіювання або підміна чипу;

– скіммінг (зчитування без прямого доступу до паспорта);

– несанкціонований доступ до чипу паспорту;

– перехоплення інформації при обміні з терміналом.

Серед механізмів, що забезпечують захист від наведеного переліку загроз, необхідно назвати такі:

– пасивна автентифікація – для захисту від компрометації змісту об'єкту захисту документу і логічної структури даних;

– активна автентифікація – для захисту від точного копіювання або підміни чипу;

– базовий контроль доступу – для захисту від скіммінгу і перехоплення інформації при обміні з терміналом;

– розширений контроль доступу – для захисту від несанкціонованого доступу;

– шифрування даних – для захисту додаткових біометричних параметрів.

Аналіз показує, що вказані механізми перше за все базуються на застосуванні асиметричних та симетричних криптографічних перетворень. Зважаючи на це, однією з основних вимог є те, що захист даних електронного паспорта має визначатися розширеним контролем доступу (EAC). Специфікації ICAO не визначають вимог, як має бути реалізований EAC, залишивши вирішення цієї проблеми на кожну окрему країну. Європейський союз визначив вимоги тільки в частині набору протоколів для реалізації EAC (доступу до критичних даних (біометричних даних) в своїх електронних паспортах (ЕП, ePassport)). Але при цьому всі країни ЄС та країни, що хочуть взаємодіяти з країнами ЄС, мають прийняти та реалізувати визначені протоколи.

Стандарти ICAO рекомендують застосовувати два механізми перевірки електронного паспорту – пасивну та активну автентифікацію [1-6]. Пасивна автентифікація є обов'язковою і призначена для автентифікації даних, які зчитані з електронного паспорту, шляхом перевірки підпису на зчитаних даних, використовуючи відповідний сертифікат ЦСК країни, що випустила паспорт. Активна автентифікація є необов'язковою і може використовуватися для перевірки чипу на справжність (автентичність). В будь-якому випадку дані, які оптично зчитані із машино зчитувальної зони, повинні порівнюватися з даними, що зчитані з чипа, для того, щоб впевнитися, що чип відповідає даному паспорту.

Базовий контроль доступу повинен дозволяти системі перевірки IS зчитувати дані з чипа тільки після доказу того, що система перевірки має право на фізичний доступ до паспорту. При цьому повинен використовуватись протокол запиту-відповіді з використанням даних з машино зчитувальної зони MRZ. Для захисту від перехоплення даних, що циркулюють між ЕП і IS, повинне використовуватись шифрування з використанням ключів сеансу.

Розширений контроль доступу призначений для обмеження доступу до критичних даних

для систем перевірки. Для одержання доступу до критичних даних система перевірки повинна довести, що вона володіє спеціальним ключем для конкретного паспорту. Цей ключ не може бути зчитаний з MRZ і потребує попереднього знання системою перевірки додаткової інформації.

Розглянемо існуючі та перспективні протоколи та механізми автентифікації електронного паспорту особи.

2. БАЗОВИЙ КОНТРОЛЬ ДОСТУПУ (BASIC ACCESS CONTROL)

Базовий контроль доступу є механізмом автентифікації і призначений для захисту персональних даних [4]. Цей механізм запобігає скіммінгу (зчитування інформації через безконтактний інтерфейс без згоди власника паспорта) та перехоплення передачі повідомлень між MRTD і системою перевірки, при використанні інформації MRTD для встановлення зашифрованого каналу передачі.

Досвід застосування електронного паспорту показує, що вразливим місцем у сучасних MRTD системах є безконтактний інтерфейс для передачі даних. Порівняння MRTD, оздобленого безконтактною інтегральною схемою, зі звичайним MRTD, свідчить про дві відмінності:

• дані, що зберігаються на чипі, можна зчитати за допомогою електронного пристрою, не відкриваючи документу (скіммінгу).

• передача незашифрованих даних між чипом і пристроєм для зчитування інформації може бути перехоплена на відстані.

Незважаючи на наявність можливих заходів фізичного захисту від скіммінгу, вони не вирішують проблеми перехоплення. У зв'язку з цим електронні паспорти другого покоління повинні бути оснащені механізмом базового контролю доступу, тобто механізм контролю доступу, фактично вимагає, щоб власник MRTD знав про те, що дані, які зберігаються на чипі, зчитуються безпечним способом. Такий механізм базового контролю доступу знижує ймовірність проведення успішного скіммінгу, а також запобігає перехопленню.

Незважаючи на те, що згідно нормативній базі ICAO механізм базового контролю доступу є додатковим, сучасний етап розвитку електронних проїзних документів вимагає його обов'язкового використання, тому всі зразки електронних паспортів другого покоління підтримують його. Базовий контроль доступу використовується для взаємної автентифікації системи перевірки і чипа MRTD, а також для встановлення ключів при забезпеченні безпечного обміну повідомленнями. Крім того, використання базового контролю доступу є обов'язковою умовою для впровадження розширеного контролю доступу – механізму, що забезпечує захист від несанкціонованого доступу до додаткових біометричних даних.

Базовий контроль доступу забезпечує можливість зчитування змісту чипа тільки після свідомого надання MRTD його власником системі, що здійснює перевірку. Чип, захищений механізмом базового контролю доступу, відмовляє у наданні доступу до свого змісту, якщо система перевірки не може підтвердити знання даних, необхідних для автентифікації. Цей доказ надається за протоколом «запит-відповідь», відповідно до якого система перевірки доводить знання індивідуальних базових ключів доступу до даного документу на чипі (K_{ENC} і K_{MAC}), які виробляються з інформації в MRZ. Система перевірки повинна бути забезпечена цією інформацією до зчитування даних з чипа. Ця інформація знімається оптично/візуально з MRTD (наприклад, з MRZ). "Інформація MRZ", складається з конкатенації номера документу, дати народження та дати закінчення терміну дії, включаючи відповідні контрольні цифри в машино зчитувальній зоні, використовуючи зчитувач знаків OCR-B . На рис. 2 наведена сторінка паспорту з особистими даними власника та машино зчитувальною зоною.

Рис. 2. Сторінка паспорту з машино зчитувальною зоною

Як альтернатива, потрібна інформація може бути вдрукована. В цьому випадку вона повинна вдруковуватися в тому вигляді, в якому фігурує в MRZ. 16 найбільш значимих байтів алгоритму хешування (SHA-1) цієї "інформації MRZ" використовуються в якості початкового заповнення генератора ключів. Це робиться з метою встановити базові ключі доступу до документа, використовуючи механізм встановлення ключів. Розглянемо його детально.

32-бітний лічильник C використовується для виведення декількох ключів з одного початкового числа. Залежно від того, чи використовується ключ для шифрування або для обчислення коду автентифікації MAC, повинні використовуватися такі значення:

– C = 1 (тобто '0 x 00 00 00 01 ') для шифрування;

– C = 2 (тобто '0 x 00 00 00 02 ') для обчислення MAC.

Для виведення двох 3DES ключів з початкового числа Kseed і C виконуються наступні етапи.

1. Нехай D є конкатенації Kseed і C (D = Kseed || C).

2. Обчислити H = SHA-1 (D), SHA-1 хеш D.

Байти 1 .. 16 з 20 байтів (160 біт) інтерпретуються як виведені з геш-функції байти з прямим порядком проходження.

3. Байти 1 .. 8 H використовуються для формування ключа Ka, а байти 9 .. 16 H для формування ключа Kb.

4. Скорегувати біти парності ключів Ka і Kb для формування правильних DES ключів.

Наведені вище етапи проілюстровані на рис. 3.

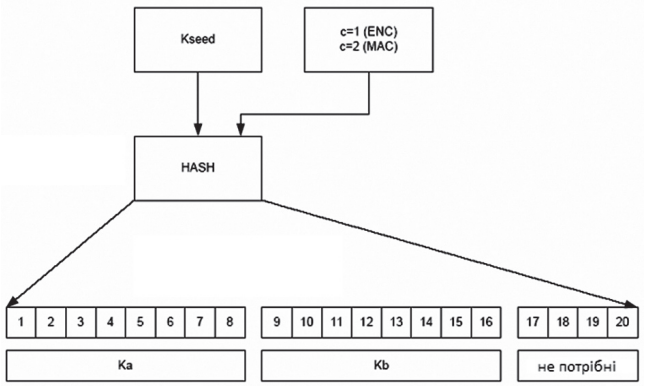


Рис. 3. Виведення двох 3DES ключів

Далі, в механізмі автентифікація і встановлення ключів забезпечуються трьох прохідним протоколом "запит-відповідь" відповідно до механізму встановлення ключів 6 стандарту ISO 11770-2 з використанням 3DES як блочного шифру. Криптографічна контрольна сума згідно MAC алгоритмом 3 ISO / IEC 9797-1 обчислюється і додається до шифр-тексту.

IFD і ICC конкретно виконують наступні етапи:

1) IFD запитує RND.ICC, посилаючи команду GET CHALLENGE. ICC генерує і відповідає спеціальним значенням RND.ICC.

2) IFD виконує наступні операції:

a) генерує спеціальне значення RND.IFD і ключовий матеріал K. IFD;

b) генерує конкатенацію S = RND.IFD | | RND.ICC || K. IFD;

c) обчислює криптограму E_IFD = E [K_ ENC] (S);

d) обчислює контрольне число M_IFD = MAC [K_MAC] (E_IFD);

e) посилає команду MUTUAL AUTHENTICATE з використанням даних E_IFD || M_IFD;

3) ICC виконує наступні операції:

a) перевіряє контрольну суму M_IFD криптограми E_IFD;

b) розшифровує криптограму E_IFD;

c) витягує RND.ICC з S і перевіряє, чи видало IFD правильне значення;

d) генерує ключовий матеріал K. ICC;

e) генерує конкатенацію R = RND.ICC | | RND.IFD || K. ICC;

f) обчислює криптограму E_ICC = E [K_ENC] (R);

g) обчислює контрольне число M_ICC = MAC [K_MAC] (E_ICC);

h) посилає відповідь з використанням даних E_ICC || M_ICC.

4) IFD виконує наступні операції:

a) перевіряє контрольну суму M_ICC криптограми E_ICC;

b) розшифровує криптограму E_ICC;

c) витягує RND.IFD з R і перевіряє, чи видало ICC правильне значення.

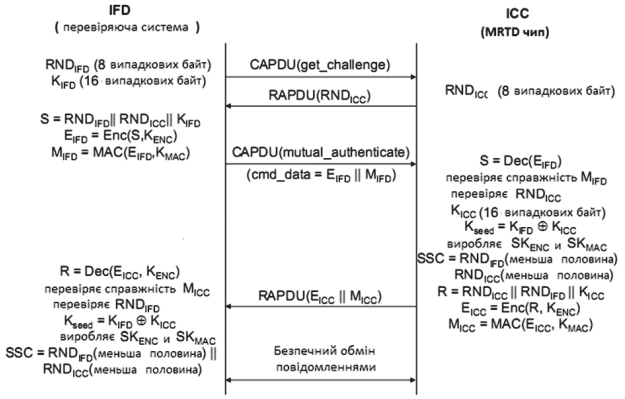


Рис. 4. Етапи виконання протоколу базового контролю доступу

Припущення про те, що базові ключі доступу до документа (K_{ENC} і K_{MAC}) не можуть бути отримані з нерозкритого документа (оскільки вони витягуються з оптично зчитуємого MRZ), дозволяє припускати, що паспорт свідомо надано для перевірки.

Крім того, після успішної автентифікації системою перевірки, потрібно, щоб чип забезпечив шифрування каналу передачі даних між системою перевірки і чипом MRTD для забезпечення методу безпечного обміну повідомленнями (Secure messaging). Вся подальша передача даних повинна захищатися методом безпечного обміну повідомленнями.

Захист від скіммінгу ґрунтується на тому, що віддалений об'єкт, який намагається зчитати інформацію, не буде мати доступу до даних у паспорті до тих пір, поки документ не буде фізично відкритий і відсканований системою перевірки.

Захист від прослуховування ґрунтується на зашифруванні каналу зв'язку за допомогою використання механізму безпечної передачі даних (secure messaging), який забезпечує зашифрування повідомлень між системою перевірки та чипом способом, який вимагає знання ключів, вироблених з "Інформації MRZ" для їх розшифровки .

Проте, важливою загрозою безпеки, закладеної в самій реалізації механізму базового контролю доступу, є відносно низька ентропія. Так як базові ключі доступу, генеруються з дев'яти знакового номера документа, дати народження та дати закінчення терміну дії, у MRTD з терміном дії десять років ентропія максимум становить [4,5]:

• 56 біт, для документів використовують тільки цифри ($365^2 * 10^{12}$)

• 73, для документів використовують цифри і букви ($365^2 * 36^9 * 10^3$)

Проблематичним є другий випадок, для якого необхідно, щоб номер документу був обраний випадково і рівномірно. При наявності додаткових відомостей (наприклад, приблизний вік власника паспорта або зв'язок між номером документа і датою закінчення терміну дії) ентропія знижується ще більше. Внаслідок відносно низькою ентропії, зловмисник може перехопити зашифрований сеанс і обчислити ключ автентифікації.

Базовий контроль доступу був введений у дію у 2004 році. Це означає, що проїзні документи, випущені в даний час (за умови, що термін дії буде становити 10 років) до кінця свого використання будуть захищені 16-річним механізмом захисту. Якщо врахувати результати застосування до протоколу базового контролю доступу закону Мура, то можна зробити висновок, що необхідно знайти альтернативу даному механізму .

3. ДОДАТКОВИЙ КОНТРОЛЬ ДОСТУПУ

Для підвищення рівня безпеки на додаток до базового контролю доступу необхідно впровадити додатковий контроль доступу. Такий протокол контролю грунтується на механізмі контролю доступу PACE (Password Authenticated Connection Establishment) [7, 8].

Цей механізм схожий на Базовий контроль доступу і також забезпечує санкціонований доступ до змісту чипа і встановлює механізм безпечного обміну повідомленнями між чипом і системою перевірки. Для встановлення безпечного обміну повідомленнями використовується короткий пароль. У протоколі PACE ентропія пароля (-ів), що використовуються для автентифікації системи перевірки, має набагато менший вплив на формування ключів і тому може бути малою.

Протокол PACE є протоколом автентифікації, заснованим на використанні пароля і представляє собою протокол встановлення ключів Діффі-Геллмана, що забезпечує безпечне підключення і засновану на паролі явну автентифікацію чипа MRTD і терміналу (тобто чип паспорта і термінал розділяють один пароль p).

Проведемо аналіз цього протоколу.

Термінал системи перевірки і чип паспорта зокрема виконують такі дії.

1. Чип MRTD випадково і рівномірно вибирає спеціальне значення s, зашифровує його як z = E (Kπ, s), де Kπ = KDFπ (π) виробляється з поділюваного паролю π. Результат – зашифроване повідомлення z разом зі статичними параметрами домену D_{PICC} терміналу.

2. Термінал відновлює відкритий текст s = = D (Kπ, z) за допомогою поділюваного пароля π.

3. І чип MRTD, і термінал виконують наступні кроки:

а) Вони обчислюють короткочасні параметри домену $D'=Map(D_{PICC},s)$.

б) Виконують анонімну процедуру встановлення ключів відповідно до протоколу Діффі-Геллмана, засновану на короткочасних параметрах домену та генерують загальний секрет $K=KA(SK_{PICC}', PK_{PCD}', D')=KA(SK_{PCD}', PK_{PICC}', D')$.

Протягом виконання протоколу Діффі-Геллмана кожна сторона перевіряє, що два відкритих ключа PK_{PICC}' и PK_{PCD}' різні.

в) Виробляють сеансові ключі $K_{MAC}=KDF_{MAC}(K)$ та $K_{ENC}=KDF_{ENC}(K)$.

г) Обмінюються і перевіряють токени $T_{PCD} = MAC(K_{MAC} , PK_{PICC}')$ та $T_{PICC} = MAC(K_{MAC}, PK_{PCD}')$.

Етапи виконання протоколу проілюстровані на рис. 5:

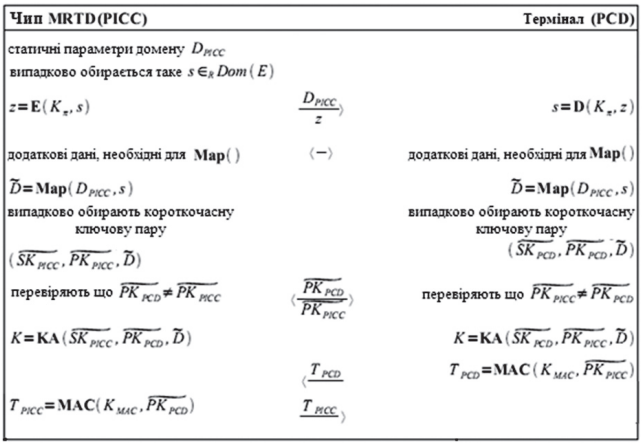


Рис. 5. Протокол PACE

Якщо PACE успішно виконаний, чип MRTD перевірив використаний пароль. Далі з використанням вироблених ключів сеансу K_{MAC} і K_{ENC} здійснюється безпечний обмін повідомленнями (Secure Messaging).

Вище приведена загальна схема виконання протоколу. Тепер проведемо більш детальний аналіз операцій, що виконуються в протоколі, використовуючи найбільш перспективний варіант, в якому криптографічні перетворення виконуються в групі точок еліптичних кривих.

Спочатку в протоколі PACE чип передає групові дані $\hat{g}$ і випадкове значення *s*, зашифровані за допомогою (геш-значення) паролю. Одержувач може повертати це значення з відповідним паролем. Потім обидві сторони беруть участь в інтерактивному протоколі Map2Point для відображення s у випадковий груповий елемент $\hat{G}$. Далі цей генератор використовується для узгодження ключа Діффі-Геллмана(DH), тобто для отримання загального ключа *K*. Як тільки цей ключ узгоджений, сторони виробляють ключі шифрування та автентифікації шляхом гешування *K*, відповідно.

У нормативних документах німецького відомства [], що відповідає за захист інформації, рекомендується використовувати наступний протокол Map2Point. Обидві сторони виконують інший DH протокол ключового узгодження (з використанням чипу для першого кроку), спільно генеруючи випадковий груповий елемент *H*, але де секретний *s* не використовується при обчис-

леннях. Потім обидві сторони обчислюють вихідні дані цього кроку як $\hat{G}$=sG+H. Позначимо цю процедуру надалі як DH2Point.

Нехай $\hat{H}$ буде геш – функцією, *C* буде блоковим шифром, і μ буде MAC. Використаємо $C(K; s)$ і $C^{-1}(K; s)$ для позначення шифрування і розшифрування *s* і *z*, відповідно, для секретного ключа *K*. Нехай $\hat{g} = (b, p, q, G, k)$ буде описом еліптичної кривої $y^2 = x^3 + ax + b \bmod p$, де $\langle G \rangle$ – група простого порядку q. Чип (A) і термінал (B) розділяють секретний пароль π із словника з N елементами, випадково вибраними, і використовують деяке відображення для генерації секретного ключа K_π для блокового шифру з π. Нижче ми приймемо $K_\pi = \hat{H}(\pi \| 0)$. Відмітимо, що ми неявно припускаємо, що сторони знають правильний пароль підчас участі у взаємодії, наприклад, користувач може вводить PIN у пристрій зчитування або термінал, який оптично сканує машинночитальну зону паспорта. Версія протоколу PACE над еліптичною кривою надана на рис. 6.

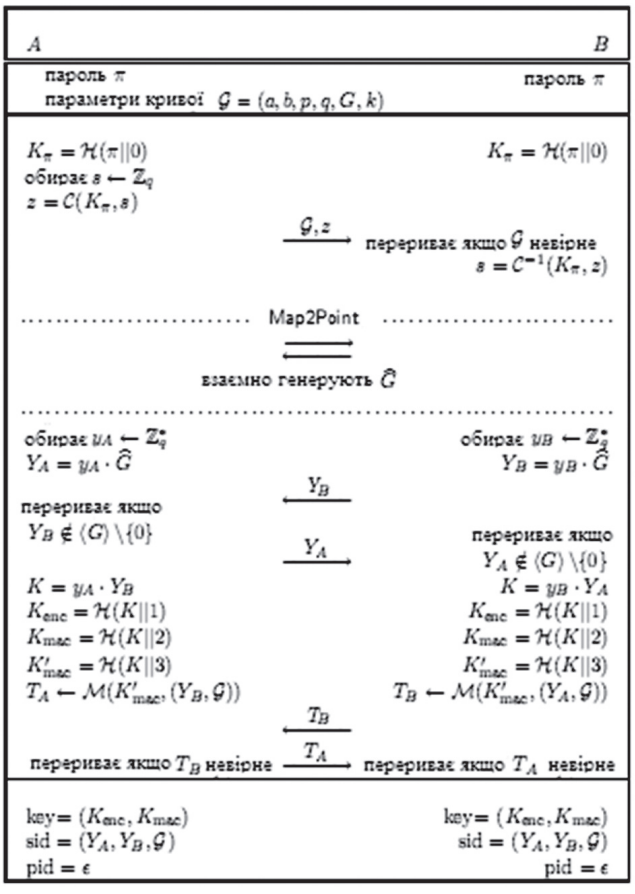


Рис. 6. DH-Заснований PACE над еліптичними кривими (з типовим Map2Point протоколом)

Опишемо можливі реалізації для Map2Point підпрограми. Припустимо, що обидві сторони перевіряють правильний формат прийнятих значень, наприклад, що H – груповий елемент.

DH2Point відображення засноване на ключовому узгодженні Діффі- Геллману. Обидві сторони генерують DH ключ H (щодо генератора *G* в $\hat{g}$) шляхом обміну $X_A = x_A G$ і $X_B = x_B G$ і приймаючи $H = x_A x_B G$. Потім s «додається» до цього ключа DH через $\hat{G}$=sG+H. Відмітимо, що сторони повинні також перевірити, що H≠0, інакше кінцеві вихідні дані повинні детерміновано залежать тільки від s.

Coin2Point відображення, засноване на киданні монети. Також створює $\hat{G}$ як $\hat{G}$ = sG+H, але обидві сторони використовують протокол кидання монети для генерування випадкового елементу H. А саме, сторона *A* спочатку генерує $X_A = x_A G$ і посилає геш-значення $\hat{H}(X_A)$, отримане з X_A, і потім сторона B передає $X_B = x_B G$. Нарешті A виявляє X_A для B (яка перевіряє, що це значення відповідає початковому геш значенню). Обидві сторони встановлюють $H = X_A + X_B$.

Hash2Point, заснований на відображенні геш – значення в точку еліптичної кривої. Припустимо, що ми маємо ефективну функція $x \rightarrow$ hash2curve(x), що дозволяє перевести рядок x до кривої безпосередньо. Потім дві сторони можуть генерувати $\hat{G}$ як вказано нижче. Далі сторона B присилає інше випадкове t (після отримання s), і нарешті обидві сторони застосовують псевдовипадковий генератор R(s, t) для того, щоб виробити x. $\hat{G}$= hash2curve(R(s, t)).

Power2Point, заснований на відображенні ступеня в групу. Цей метод може застосовуватись тільки для груп над Z^*p. При його реалізації сторони використовують функцію $s \rightarrow s^w \bmod p$ для $p = wq + 1$ для w з великими простими чинниками тільки для відображення s в елемент підгрупи Z^*p. Той факт, що w не має малих чинників, гарантує статистичну близькість відображення до однорідного (за умови, що значення s однорідне). Можна знову скомбінувати це відображення з інтерактивним генеруванням H, або з методом перешифрування. Описані вище варіанти реалізації складової частини протоколу наведені на рис. 7.

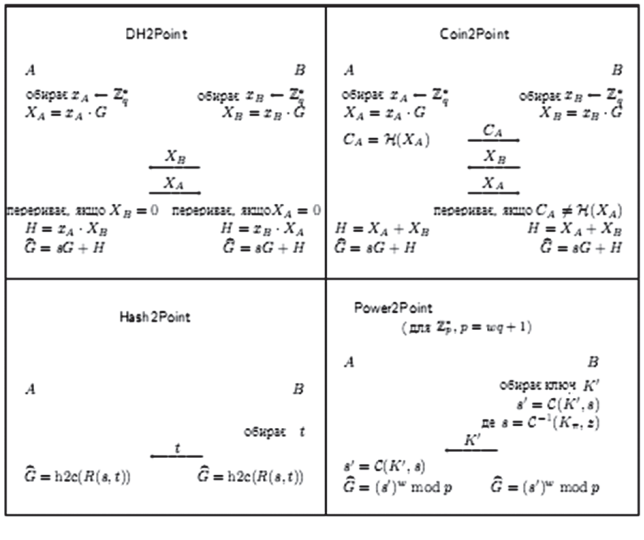


Рис. 7. Варіанти виконання складової частини протоколу Map2Point

Існують різні варіанти паролів, які можуть використовуватися в системі PACE.

Першим варіантом паролю є використання інформації з MRZ. Цей варіант забезпечує сумісність і представляє собою інформацію про номер документу, дати народження й дата закінчення терміну дії, зчитану оптично з розкритого паспорту (також як у базовому контролі доступу). Пароль MRZ може бути використаний тільки для додатків ePassport (як для BAC, так і для PACE). Цей пароль є статичним симетричним ключем, що не може бути заблокованим.

Другим варіантом, що описаний у публікаціях ICAO[], є механізм CAN (Card Access Number), який припускає, що номер друкується на сторінці з даними або на лицьовій стороні картки TD1. Виходячи з цього, CAN може бути відносно коротким (6 цифр в загальному випадку достатньо). Це є перевагою, оскільки він легко може бути надрукований вручну. Пароль CAN може бути використаний для доступу до всіх програм на чипі MRTD (ePassport, eID, і eSign). Цей пароль також є ключем, що не може бути заблокованим, тобто чип MRTD не повинен блокувати CAN після невірної автентифікації. CAN може бути статичним (надрукованим на MRTD), наполовину статичним (наприклад надрукованим на наклейці на MRTD) або динамічним (випадково вибиратися чипом MRTD і відображатись на MRTD з використанням ePaper, OLED або подібних технологій) [1-5].

Крім того, існує можливість використання таких видів паролів, які не внесені в попередні рекомендації ICAO, але мають можливість з'явиться в кінцевих технічних описах. До них відносяться PIN і PUK [6-8].

PIN (Personal Identification Number) – короткий секретний пароль, який повинен бути відомий тільки легітимного власнику документу. Він може бути використаний для доступу до додатків eID. Використання PIN рекомендується для всіх терміналів автентифікації, оскільки тільки легітимний власник може дозволити терміналу доступ до даних, що зберігаються в eID додатках. PIN є паролем, що може бути заблокованим, тобто PIN пов'язаний з лічильником спроб (RC), який зменшує своє значення після кожної не дійсної автентифікації. Така процедура забезпечує захист чипу MRTD від DOS атак.

Якщо RC = 1: чип MRTD призупинятиме PIN, тобто чип MRTD повинен відкидати спроби автентифікації до тих пір, поки PIN не буде продовжений. Для продовження виконання PIN повинен бути введений коректно. PIN має бути введений в одній сесії, в іншому випадку (наприклад після вимкнення живлення) PIN буде залишатися призупинення. Лічильник RC буде встановлюватися відповідно до введеному PIN:

• якщо PIN введено правильно, то зчитувач RC скидається до вихідного значення.

• якщо PIN введено невірно, то лічильник зменшується до значення RC = 0.

Якщо RC = 0, то чип MRTD заблокує PIN, тобто чип MRTD не повинен приймати ніякі подальші спроби автентифікації з використанням заблокованого PIN. Для розблокування PIN необхідно перезавантажити лічильник, використовуючи процедуру розблокування, і при можливості встановлення нового PIN.

PUK (PIN Unblock Key) – достатньо довгий секретний пароль, який повинен бути відомий тільки легітимного власнику документа. Він використовується тільки для процедури розблокування PIN.

Хоча криптографічні протоколи різні, проте процедура перевірки, коли проїзний документ, що пред'являється системі перевірки, оздоблений додатковим контролем доступу, така ж як і у базовому протоколі доступу. Оптично або візуально зчитується інформація, що використовується для вироблення ключів PACE, на яких отримується доступ до чипу та здійснюється протоколу Безпечного обміну інформацією між чипом паспорта та системою перевірки.

З метою збереження взаємодії різних систем, додатковий контроль доступу визначається як механізм, що доповнює базовий контроль доступу. Тому він може бути впроваджений у доповнення до нього, але не замість нього. Базовий контроль доступу буде залишатися «протоколом за замовчуванням» до тих пір, поки він буде забезпечувати достатню безпеку. Аналіз показує, що поступовий перехід від BAC до PACE передбачається протягом 10-20 років. Протягом найближчих 5 років проїзні документи і системи перевірки повинні почати підтримувати механізм додаткового контролю доступу. Розширений контроль доступу в другій версії повинен бути використаний разом з PACE замість базового контролю доступу.

На останній 19 конференції Технічної консультативної групи з питань машино зчитувальних проїзних документів ICAO, яка пройшла 7-9 грудня 2009 року, особливу увагу було приділено питанням впровадження механізму додаткового контролю доступу. Більшість делегатів даної конференції зійшлися на думці, що перед внесенням даного механізму в специфікації ICAO і його впровадженням, необхідно провести його глибокий комплексний аналіз.

ВИСНОВКИ

На сьогоднішній день існує два варіанта механізму базової автентифікації. Цими механізмами є базовий контроль доступу, який детально описаний в нормативних документах ICAO, та механізм додаткового контролю доступу, який на даному етапі перебуває в процесі аналізу та опрацюванні фахівцями технічно консультативну групу з машино зчитувальних проїзних документів та робочої групи з новітніх технологій. Результатом цього аналізу, судячи за все, стане прийняття цього механізму як можливого до використання в проїзних документах.

При детальному аналізі механізму базового контролю доступу встановлено, що в самій реалізації механізму базового контролю доступу існує важлива загроза безпеці – відносно низька ентропія. Внаслідок відносно низькою ентропії, зловмисник може перехопити зашифрований сеанс і обчислити ключ автентифікації. Якщо врахувати результати застосування до протоколу базового контролю доступу закону Мура, то можна зробити висновок, що з плином часу захист буде не достатнім.

Додатковий контроль доступу схожий на базовий контроль доступу і також забезпечує санкціонований доступ до змісту чипа і встановлює механізм безпечного обміну повідомленнями між чипом і системою перевірки. Протокол ґрунтується на механізмі контролю доступу PACE (Password Authenticated Connection Establishment). Для встановлення безпечного обміну повідомленнями використовується короткий пароль. У протоколі PACE ентропія пароля (-ів), що використовуються для автентифікації системи перевірки, має набагато менший вплив на формування ключів і тому може бути дуже малою.

Механізм додаткового контролю доступу (SAC) (який функціонує ґрунтуючись на використанні протоколу PACE), зберігає все функціональне навантаження, яким володіє механізм базового контролю доступу (BAC), та в той самий час позбавлений його основного недоліку – низької ентропії.

Література.

[1] ICAO 9303- 9303 part 1 volume 1, Sixth edition, 2006, Passports with MachineReadable Data Stored in Optical Character Recognition Format

[2] ICAO 9303- : 9303 part 1 volume 2, Sixth edition, 2006, Specifications for Electronically Enabled Passports with Biometric Identification Capability

[3] ICAO NTWG. Technical report. PKI for Machine Readable Travel Documents offering ICC Read-Only Access; Version – 1.1; October 01, 2004

[4] Common Criteria Protection Profile – Machine Readable Travel Document with„ICAO Application", Basic Access Control, reference : BSI-PP-0017, Version 1.0, 18thAugust 2005, BSI.

[5] Security and Privacy Issues in E-passports, By Ari Juels, David Molnar, and David Wagner

[6] Technical Report Supplemental Access Control Technical advisory group on machine readableTravel documents (tag-mrtd) Nineteenth meeting Montrйal, 7 to 9 december 2009

[7] BSI TR-03110, "Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, 2010

[8] J. Bender, M. Fishlin, D. Kuegler, "Security Analysis of the PACE Key-Agreement Protocol", Information Security Conference (ISC) 2009, Lecture Notes in Computer Science, Volume 5735, pp. 33-48, Springer-Verlag, 2009.

Надійшла до редколегії 8.06.2010.

Горбенко Юрій Іванович, канд. техн. наук, технічний директор ЗАТ «ІІТ». Область наукових інтересів: дослідження механізмів системи електронних цифрових паспортів.

Тоцький Олександр Сергійович, начальник відділу тестування та вихідного контролю ЗАТ «ІІТ». Область наукових інтересів: дослідження механізмів системи електронних цифрових паспортів.

Повтарєв Дмитро Валерійович, студент групи ІБ-06-2 ХНУРЕ. Область наукових інтересів: дослідження механізмів системи електронних цифрових паспортів.

УДК 004.056.52:004.057.4

Механизмы и протоколы автентификации электронного паспорта / Ю.И. Горбенко, Д.В. Повтарев, А.С. Тоцкий // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 378–385.

Приведены результаты анализа протоколов базовой аутентификации электронного паспорта лица. Приведен их краткое описание и предоставлены рекомендации по выбору механизма для внедрения в модель загранпаспорта гражданина Украины.

Ключевые слова: электронный паспорт, аутентификация, базовый контроль доступа.

Ил. 07. Библиогр.: 8 назв.

UDC 004.056.52:004.057.4

Authentication mechanisms and protocols for person's e-passport / Yu.I. Gorbenko, D.V. Povtarev, O.S. Totskiy // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 378-385.

The results of analyzing the basic authentication protocols for a person's e-passport are given . Their brief description is given and recommendations on choosing a mechanism for implementing into a citizen of Ukraine's foreign passport model are provided.

Keywords: e-passport, authentication, basic access control.

Fig. 7. Ref.: 8 items.

УДК 681.324.067

МЕТОД ПОБУДУВАННЯ ВИПАДКОВИХ БІТІВ НА ОСНОВІ СПАРЮВАННЯ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

І.Д. ГОРБЕНКО, Н.В. ШАПОЧКА, К.А. ПОГРЕБНЯК

Наводиться обґрунтування та викладається сутність і властивості генератора детермінованих випадкових бітів на основі криптографічного перетворення типу спарювання точок еліптичних кривих.

Ключові слова: еліптичні криві, детерміновані випадкові послідовності.

ВСТУП

Нині актуальною є задача криптографічного захисту інформації в різноманітних інформаційних технологіях та інформаційно – телекомунікаційних системах. Суттєво важливими складовими таких систем, від властивостей яких залежить якість надання криптографічних послуг, є засоби генерування ключів та параметрів. Існуючі методи та на їх основі засоби генерування ключів та параметрів можна розділити на два великих класи – випадкових та детермінованих випадкових послідовностей (бітів). Обидва вказані класи генераторів знаходять застосування, але більш широко використовують детерміновані генератори випадкових бітів (ДГВБ) [1], по крайній мірі в частині інтенсивності їх використання.

Також згідно рекомендацій [2] ДГВБ можна розділити на три великих групи:

– ДГВБ на основі перетворень в групі точок еліптичних кривих;

– ДГВБ на основі перетворень з використанням геш – функцій;

– ДГВБ на основі використання блокових шифрів.

Для оцінки властивостей ДГВБ рекомендується використовувати такі показниками, як [3]: період l повторення (довжина) детермінованої випадкової послідовності; основа алфавіту m ДГВБ; ймовірність перекриття в просторі або в часі двох сегментів Y_r та Y_μ; структурна скритність (еквівалентна складність) S_e ДГВБ Y; ентропія $H_k(N_k)$ джерела ключів для випадку, коли генератор детермінованих випадкових послідовностей використовується як джерело ключів; відстань рівнозначності l_0 конкретної послідовності Y_v; безпечний час генератора детермінованих випадкових послідовностей t_b; складність I_y формування послідовності Y; довжина параметрів зворотного зв'язку B_2 та властивості випадковості, рівноймовірності, незалежності та однорідності.

За всіма названими показниками до детермінованого генератора випадкових бітів повинен бути пред'явлений ряд вимог [4]. Так, період повторення повинен бути $l_n \geq l_z$, тобто не менше заданого, основа алфавіту m, ймовірність перекриття $P_n < P_z$ менше допустимої, структурна скритність $S \geq S_g$, ентропія джерела ключів $H \geq H_g$, відстань рівнозначності $l_0 > l_g$, безпечний час $t_b > t_g$, тобто не менш допустимих. Крім того, реалізація Y_i повинна задовольняти вимогам випадковості, рівноймовірності, незалежності та однозначності, а також забезпечувати генерування бітів з необхідною швидкодією.

Проведений аналіз показав, що ДГВБ, які засновані на геш – функціях, мають ряд переваг [4]. Так ДГВБ можуть використовувати будь-яку ISO/IEC криптографічну геш – функцію із ISO/IEC 10118-3 за умови забезпечення достатньої ентропії для початкового значення. Але для таких генераторів необхідно генерувати, в тому числі згідно ключа, символи прообразів з довільним алфавітом послідовності прообразу, завідомо заданим періодом повторення l, допустимою швидкодією (складністю) генерування символів та криптографічною стійкістю проти визначення закону генерування ДГВБ.

Метою цієї статті є обґрунтування можливості, визначення умов побудування, дослідження різних варіантів побудування та розробка рекомендацій відносно застосування ДГВБ, у якого символи прообрази генеруються на основі спарювання точок еліптичних кривих у вигляді елементів підгрупи розширення поля, а безпосередньо символи образи на основі обчислення геш – значень від символів прообразів.

1. МЕТОД ГЕНЕРАЦІЇ ВИПАДКОВИХ БІТІВ НА ОСНОВІ СПАРЮВАННЯ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

Ідея побудування ДГВБ базується на основній властивості скалярного відображення – його білінійності або властивості спарювання [5]. Вона полягає в тому, що для деяких точок еліптичної кривої B і D над полем F_g, а також цілих a та c є справедливим таке:

$$K = Спарювання(a \bullet B, c \bullet D) = \\ = Спарювання(c \bullet B, a \bullet D). \quad (1)$$

В результаті спарювання точок B та D отримуємо елемент мультиплікативної підгрупи розширення поля F_{q^i}, де i ціле та може приймати значення на відрізку (2, 6).

Ідея побудування ДГВБ полягає в тому, щоб на першому етапі за деяким методом (алгоритмом) спарювання генерувати послідовність елементів мультиплікативної групи розширення поля F_{q^i}, а

на другому від кожного такого елементу обчислювати геш – значення, використовуючи певну геш – функцію.

На рис. 1 зображено функціональну схему (алгоритм) ДГВБ на основі спарювання точок еліптичних кривих. Перед початком роботи ДГВБ необхідно встановити в початковий стан, скажемо m. Оскільки ми розглядаємо генератор бітів, то число станів можна приблизно оцінити як . Як правило m повинне бути випадковим, хоча при деяких умовах m може генеруватись і за допомогою іншого ДГВБ. Перед введенням m-бітне початкове число розбивається навпіл і в подальшому використовується в якості x-координат точок на еліптичній кривій, і, таким чином, задаючи випадково x-координати випадково задаються 2 точки еліптичної кривої.

Генерування випадкового елементу мультиплікативної підгрупи розширення поля F_{q^i} здійснюється таким чином. Два випадкових значення t вводяться в елемент $\varphi(x)$, причому t значення може модифікуватись під впливом додаткових даних та/або зворотних даних y. Перетворення $x(t)$ перевіряє x-координату на її приналежність еліптичній кривій, а $\varphi(x)$ знаходить y-координату точки відповідно до значення x шляхом вирішення рівняння еліптичної кривої.

Таким чином, випадково формуються дві точки еліптичної кривої $P(x,y)$ та $Q(x,y)$. Далі ці дві точки спарюються згідно перетворення Вейля [6]. В результаті спарювання формується перший елемент мультиплікативної підгрупи a_1, в подальшому генеруються наступні елементи підгрупи. Зразу відмітимо, що існує можливість рекурентного формування усіх елементів підгрупи порядку q. Для забезпечення необхідної якості випадковості далі застосовується перетворення типу гешування.

Вибір стандарту гешування та параметрів функції гешування складає окремий предмет досліджень. В процесі досліджень було обґрунтовано, що розмір елементів a_1 мультиплікативної підгрупи повинен бути не менше довжини геш-значення l_h. За таких умов, тобто коли $l_h < l_a$, будуть виникати колізії геш–значень елементів мультиплікативної групи, ймовірності виникнення яких залежать від того, наскільки $l_a > l_h$. Результати дослідження виникнення колізій наведені нижче.

Попередній аналіз наведеної схеми, а також проведене програмне моделювання показали, що перетворення спарювання Вейля має значну складність, якщо його застосовувати кожен раз при обчисленні наступного елемента мультиплікативної групи. Пропонується будувати ДГВБ, який базується на властивості білінійного спарювання.

2. ОЦІНКА ЙМОВІРНОСТІ ВИНИКНЕННЯ КОЛІЗІЙ ГЕШ-ЗНАЧЕНЬ

Проведений аналіз ДГВБ показав, що при його застосуванні можуть виникати два різних класи за природою виникнення колізій. До першого відносяться колізії, які виникають при обчисленні геш – значень за умови, що $l_a > l_h$. До другого відносяться колізії, що виникають при випадковому формуванні елементів мультиплікативної підгрупи розширення поля. Розглянемо їх послідовно, орієнтуючись на схему ДГВБ (рис. 1).

Згідно схеми ДГВБ, що наведена на рис. 1, елементи a_i мультиплікативної підгрупи порядку q гешуються з використанням колізійно стійкої геш–функції. За умови, коли $l_a > l_h$, можливі колізії геш–значень, а це означає, що відрізки випадкових бітів довжини l_h будуть співпадати. Тому розглянемо дві основні задачі оцінки колізій.

1. Нехай є деяка функція H обчислення геш-значення від елементів мультиплікативної підгрупи

$$h = H(a_i), i = 1,...,q;$$

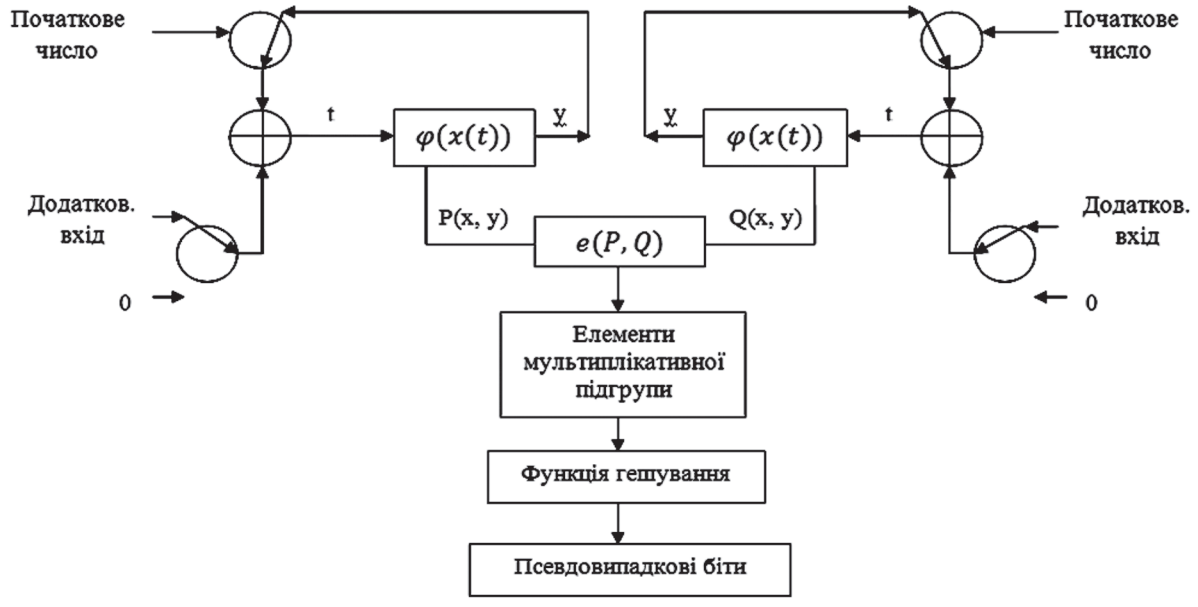


Рис. 1. ДГВБ на основі спарювання точок еліптичних кривих

причому h може приймати $n = 2^{l_h}$ значень незалежно від довжини l_a. Необхідно визначити число k випадкових елементів мультиплікативної підгрупи a_i, які необхідно подати на вхід засобу гешування, щоб з імовірністю P_k відбувся хоча б один збіг виду $H(a_i) = H(a_j)$, тобто відбулася колізія.

2. Нехай на виході засобу гешування H з повної множини значень $n = 2^{l_h}$ формуються k випадкових геш-значень функції перетворення $H(a_i)$, причому $k \le n$ і ймовірність появи h_i підкоряється рівноймовірному закону розподілу. Необхідно знайти ймовірність $P(n,k)$ того, що ці безлічі містять в собі хоча б по одному елементу x_i і y_j, такі, що $x_i = y_j$.

Важливість вирішення першої задачі пояснюється наступним. По суті k є допустимим значенням числа елементів мультиплікативної групи, при генеруванні яких колізія відбувається з ймовірністю P_k. Друга задача є оберненою першій, в ній необхідно знайти ймовірність колізії при відомих n та k.

Розв'язок виконаємо на основі узагальненого "парадоксу дня народження". В [7] показано, що ймовірність відбуття колізії $P(n,k)$ для загального випадку може бути обчислена.

$$P_k(n,k) = 1 - \frac{n(n-1)(n-2)...(n-(k-1))}{n \quad n \quad n \qquad\qquad n} =$$
$$= 1 - 1\left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right)...\left(\frac{n-(k-1)}{n}\right) = \qquad (2)$$
$$= 1 - \left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right)...\left(1 - \frac{k-1}{n}\right).$$

При реальних значеннях n та k зробити обчислення згідно формули практично неможливо. Але якщо врахувати, що в реальних випадках $k < 0{,}1n$, то для спрощення (2) можна зробити заміну $(1-x) \le e^{-x}$, в результаті маємо

$$P_k(k,n) = 1 - e^{-\frac{1}{n}} \cdot e^{-\frac{2}{n}} ... e^{-\frac{k-1}{n}} =$$
$$= 1 - e^{-\frac{1}{n(1+2+3+...+k-1)}} = \qquad . \qquad (3)$$
$$= 1 - e^{-\frac{k(k-1)}{2n}} = 1 - e^{-\frac{k(k-1)}{2 \cdot 2^{l_h}}}$$

Таким чином, при вказаних обмеженнях одержано аналітичне співвідношення, що зв'язує між собою імовірність колізії $P_k(n,k) = P_k$, число сформованих елементів мультиплікативної підгрупи k довжиною l_h та загальне число елементів мультиплікативної групи $n = 2^{l_h}$.

Формула (3) дозволяє:

– зробити оцінку імовірності колізій P_k, розглядаючи її у залежності від k та l_h;

– визначити критичне значення в залежності від допустимого значення імовірності колізії P_k для різних величин k;

– визначити обмеження на число сформованих елементів мультиплікативної підгрупи k, при яких імовірність колізії не перевищує P_k.

При оцінці величин імовірності колізії можна використовувати вираз (3). При цьому для випадку, коли $k^2 >> k$, його можна спростити до виду

$$P_k(k,n) \approx 1 - e^{-\frac{k^2}{2^{(l_h+1)}}}. \qquad (4)$$

В таблиці 1 наведені значення ймовірностей колізії P_k в залежності від k та l_h.

Критичне значення можна знайти із співвідношень (3) або (4), подавши його у виді

$$1 - P_k = e^{-\frac{k(k-1)}{2^{l_i+1}}} = e^{-\frac{k(k-1)}{2n}}. \qquad (5)$$

Прологарифмувавши вираз(5), маємо

$$\ln(1 - P_k) = -\frac{\left(k^2 + k\right)}{2^{l_i+1}} = -\frac{\left(k^2 + k\right)}{2n}. \qquad (6)$$

Далі із (6) спочатку знаходимо як

$$n_{kp} = -\frac{\left(k^2 + k\right)}{\left(2\ln(1 - P_k)\right)}. \qquad (7)$$

Критичне значення знаходимо із виразу $n_{kp} = 2^{l_{kp}}$, отже

$$l_{kp} = \log_2 n_{kp}. \qquad (8)$$

В табл. 2 наведено значення мінімально допустимих довжин (бітів) в залежності від величин k та P_k. Але при виборі значення необхідно враховувати, що геш–значення можуть приймати тільки фіксовані довжини – 160, 256, 384 та 512 бітів.

Таблиця 1

Значення ймовірностей колізії P_k в залежності від k та l_h

l \ k	2	16	32	64	128	256	1024	65536	10^9	10^{12}
8	0,004	0,38	0,867	0,999	~1	~1	–	–	–	–
16	$3.05 \cdot 10^{-5}$	$1.9 \cdot 10^{-3}$	$7.7 \cdot 10^{-3}$	0,031	0,118	0,393	0,999	~1	–	–
32	$4{,}6 \cdot 10^{-10}$	$2{,}9 \cdot 10^{-8}$	$1{,}1 \cdot 10^{-7}$	$4{,}7 \cdot 10^{-7}$	$1{,}9 \cdot 10^{-6}$	$7{,}6 \cdot 10^{-6}$	$1{,}2 \cdot 10^{-4}$	0.393	~1	–
64	$9{,}7 \cdot 10^{-20}$	$6{,}2 \cdot 10^{-18}$	$2{,}5 \cdot 10^{-17}$	$9{,}9 \cdot 10^{-17}$	$3{,}9 \cdot 10^{-16}$	$1{,}7 \cdot 10^{-15}$	$2.8 \cdot 10^{-14}$	$1.1 \cdot 10^{-10}$	0,02	~1
128	~0	~0	~0	~0	~0	~0	~0	$1{,}7 \cdot 10^{-29}$	$1{,}2 \cdot 10^{-21}$	$1{,}2 \cdot 10^{-15}$
256	~0	~0	~0	~0	~0	~0	~0	~0	~0	~0
512	~0	~0	~0	~0	~0	~0	~0	~0	~0	~0

Обмеження на число сформованих елементів мультиплікативної підгрупи k_0, при яких імовірність колізії не перевищує P_k, можна здійснити, використавши (5). В результаті по аналогії з [7] маємо:

$$k^2 + k + 2n\ln(1-P_k) = 0. \quad (9)$$

При значенні $k^2 >> k$ можна використовувати співвідношення

$$k^2 + 2n\ln(1-P_k) = 0.$$

Тоді оцінкою величини k є значення

$$k = \sqrt{-2n\ln(1-P_k)} = \sqrt{-2^{l_h+1}\ln(1-P_k)}. \quad (10)$$

Таким чином, використовуючи наведений математичний апарат, можна зробити оцінки ймовірностей виникнення колізій геш-значень елементів мультиплікативної підгрупи a_i та вибрати довжини геш–значень, тобто вибрати допустимі значення l_h, зважаючи на те, що довжини геш–значень є стандартизованими, як уже вказувалось – 160, 256, 384 та 512 бітів. Також вирішивши параметричне рівняння (9) відносно k_0, знайдемо обмеження на число блоків випадкової послідовності бітів, що можуть бути генеровані на одному і тому ж ключі.

3. ОЦІНКА ЙМОВІРНОСТЕЙ ВИНИКНЕННЯ КОЛІЗІЙ ПРИ ВИПАДКОВОМУ ФОРМУВАННІ ЕЛЕМЕНТІВ МУЛЬТИПЛІКАТИВНОЇ ПІДГРУПИ

Тепер розглянемо другу задачу оцінки ймовірностей виникнення колізій ДГВБ при випадковому формуванні елементів мультиплікативної підгрупи a_i розширення поля порядку q. Будемо розглядати ймовірності виникнення колізій за рахунок того, що при випадковому формуванні елементів мультиплікативної підгрупи a_i можуть відбуватись події, коли відбудеться колізія в виборі одного й того ж елементу мультиплікативної підгрупи a_i. Це справедливо, якщо елементи мультиплікативної підгрупи a_i будемо вибирати випадково й рівноймовірно.

Для цього випадку ймовірність $P(n,k)$ того, що ці безлічі містять в собі хоча б по одному елементу x_i і y_j, такі, що $x_i = y_j$, можна оцінити також використовуючи λ-метод.

В нашому випадку подія $x_i = y_j$ може відбутися з ймовірністю $1/q$, де q – порядок підгрупи.

Тому ймовірність того, що $x_i \neq y_j$ обчислюється як:

$$Q(x_i \neq y_j) = 1 - \frac{1}{q}. \quad (11)$$

Якщо Y включає в себе k подій, то ймовірність того, що всі значення $y_1, y_2, .., y_k$ не співпадуть з x_i, може бути обчислена як

$$Q(x_i \neq Y) = \left(1 - \frac{1}{q}\right)^k. \quad (12)$$

Ймовірність того, що хоча б одне значення Y співпаде з x_i, є

$$R(x_i \in Y) = 1 - \left(1 - \frac{1}{q}\right)^k. \quad (13)$$

Нехай всі елементи X різні. Це справедливо, так як $k << q$, наприклад, $k = \sqrt{q}$. Тоді ймовірність того, що

$$R(x_i \notin Y) = \left(1 - \frac{1}{q}\right)^k$$

і

$$R(x \notin Y) = \left(\left(1 - \frac{1}{q}\right)^k\right)^k = \left(1 - \frac{1}{q}\right)^{k^2}. \quad (14)$$

Далі, ймовірність того, що хоча б одна подія із X і Y співпаде, є

$$R(x_i = y_j) = 1 - \left(1 - \frac{1}{q}\right)^{k^2}. \quad (15)$$

Позначимо $x = \frac{1}{q} << 1$ і скористаємося співвідношенням $(1-x) \le e^{-x}$. В результаті отримаємо

$$R(q,k) = 1 - \left(1 - \frac{1}{q}\right)^{k^2} = \left(1 - \left(e^{-1/q}\right)^{k^2}\right) = 1 - e^{-\frac{k^2}{q}}. \quad (16)$$

Таким чином, ймовірність того, що в двох множинах X і Y хоча б по одному елементу співпадуть,

$$P(q,k) = P_з = 1 - e^{-k^2/q}. \quad (17)$$

Перетворюючи (17), отримаємо

$$e^{-k^2/q} = 1 - P_з. \quad (18)$$

Логарифмуючи (18), маємо

$$-\frac{k^2}{q} = \ln(1 - P_з)$$

Таблиця 2

Значення мінімально допустимих довжин (бітів) в залежності від величин k та P_k

P_k \ k	2	8	16	32	64	128	256	1024	32768	65536	10^6	10^9	10^{12}
10^{-3}	11	15	17	19	20	22	24	28	38	40	48	68	88
10^{-6}	21	25	27	28	30	32	34	38	48	50	58	78	98
10^{-9}	31	35	36	38	40	42	44	48	58	60	68	88	108
10^{-12}	41	45	46	48	50	52	54	58	68	70	78	98	118
10^{-16}	54	58	60	62	64	66	68	72	82	84	91	111	131

і далі

$$k^2 = -q\ln\left(\frac{1}{1-P_з}\right)^{-1} = q\ln\left(\frac{1}{1-P_з}\right).$$

Наприкінці отримаємо

$$k = \sqrt{q\ln\left(\frac{1}{1-P_з}\right)}. \qquad (19)$$

Оцінимо значення ймовірностей виникнення колізій ДГВБ при випадковому формуванні елементів мультиплікативної підгрупи a_i. Обчислимо $\lim_{q\to\infty}(1-e^{\frac{-k^2}{q}}) = \lim_{q\to\infty}(1-\frac{1}{e^{\frac{k^2}{q}}})$. Так як $q\to\infty$, то $\frac{k^2}{q}\to 0$, а $e^{\frac{k^2}{q}}\to 1$. Тоді $\lim_{q\to\infty}(1-e^{\frac{-k^2}{q}}) = \lim_{q\to\infty}(1-\frac{1}{e^{\frac{k^2}{q}}})\to 0$.

4. РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ДГВБ

Для представленого вище методу генерування випадкових бітів була розроблена універсальна програмна модель ДГВБ, з використанням якої проведено його випробовування та тестування. Випробовувались та тестувались три різні варіанти реалізації генератора:

– ДГВБ реалізований таким чином, коли в якості випадкової послідовності безпосередньо використовується послідовність елементів мультиплікативної підгрупи a_i, тобто без застосування функції гешування;

– ДГВБ, що реалізований згідно рис. 1, а послідовність елементів мультиплікативної підгрупи a_i генерується рекурентно, а початковий стан генератора задається згідно діючого ключа;

– ДГВБ, що реалізований згідно рис. 1, але послідовність елементів мультиплікативної підгрупи a_i вибирається випадково (з використанням ключа), а початковий стан генератора задається згідно діючого ключа;

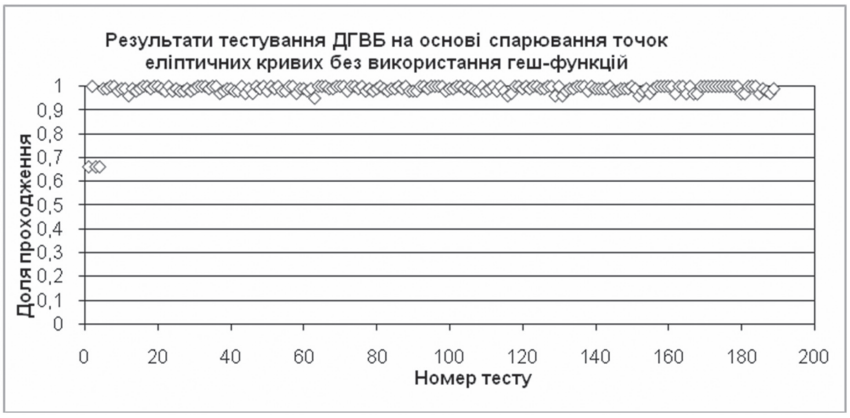
– ДГВБ реалізований таким чином, коли в якості випадкової послідовності безпосередньо використовується послідовність елементів мультиплікативної підгрупи a_i, тобто без застосування функції гешування.

В таблицях 4 та 5 наведені результати тестування ДГВБ тільки на основі спарювання точок еліптичних кривих та класичного генератора BBS[8].

В таблицях 6, 7 та 8 наведені результати тестування ДГВБ згідно рис. 1 та з застосуванням безпосереднього спарювання та гешування з використанням функції гешування SHA-2(з довжиною геш значення 256 бітів).

Таблиця 3

Результати статистичного тестування ДГВБ на основі спарювання точок еліптичних кривих без гешування з використанням NIST SP 800-22



Таблиця 4

ДГВБ на основі спарювання точок еліптичних кривих та генератор BBS

Генератор	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
ДГВБ на основі спарювання точок еліптичних кривих	133 (70,4%)	185 (97,9%)

Таблиця 5

ДГВБ на основі спарювання точок еліптичних кривих та генератор BBS з урахуванням двох значень P ($P \le 0{,}01$, $P \le 0{,}001$)

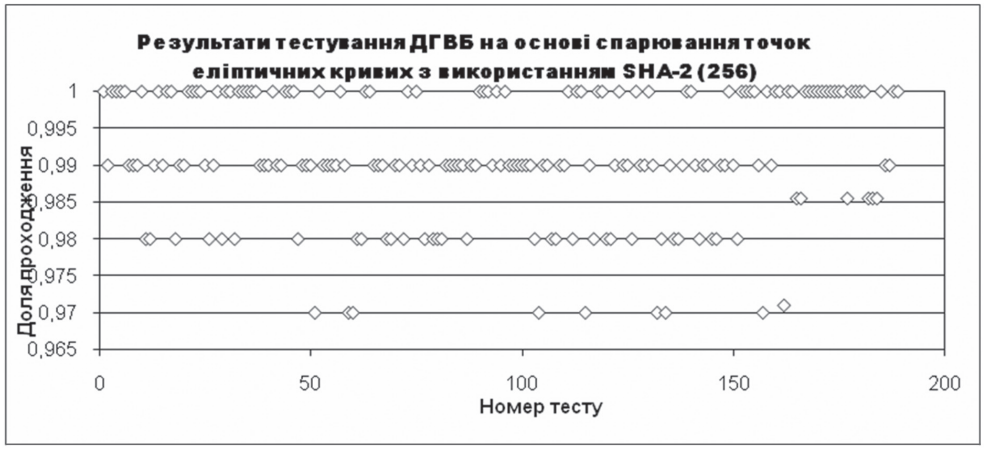
Генератор	Кількість тестів, в яких значення ймовірності $P \le 0{,}01$	Кількість тестів, в яких значення ймовірності $P \le 0{,}001$
BBS	0	0
ДГВБ на основі спарювання точок еліптичних кривих	5	3

В таблицях 9, 10 та 11 наведені результати статистичного тестування ДГВБ на основі спарювання точок еліптичних кривих без гешування з рекурентним генеруванням елементів мультиплікативної підгрупи a_i (модифікований метод).

В таблицях 12, 13 та 14 наведені результати тестування модифікованого ДГВБ згідно рис. 1 з застосуванням безпосереднього спарювання та гешування з використанням функції гешування SHA-2(з довжиною геш значення 384 бітів).

Таблиця 6

ДГВБ на основі спарювання точок еліптичних кривих з використанням SHA-2 (256)



Таблиця 7

ДГВБ на основі спарювання точок еліптичних кривих з застосуванням функції гешування та генератор BBS

Генератор	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
ДГВБ на основі спарювання точок еліптичних кривих та гешування	142 (75,1%)	189 (100%)

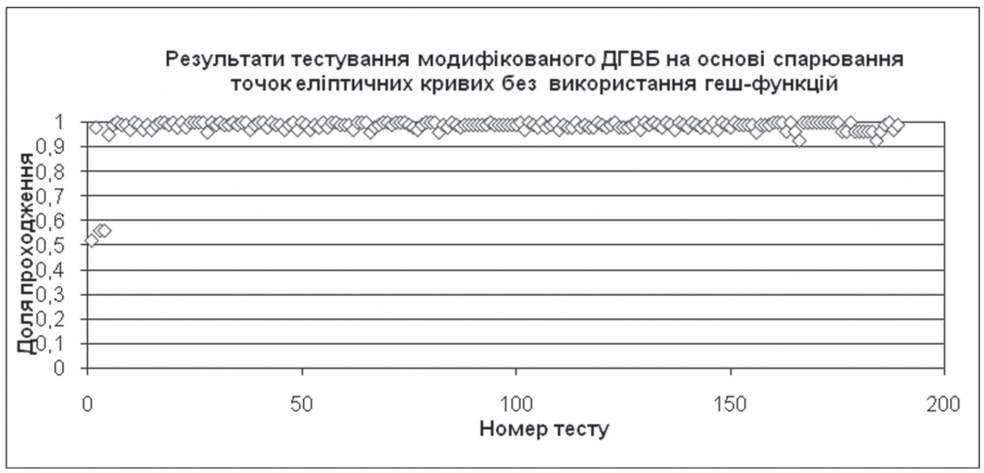
Таблиця 8

ДГВБ на основі спарювання точок еліптичних кривих з застосуванням функції гешування та генератор BBS з урахуванням двох значень P ($P \le 0{,}01$, $P \le 0{,}001$)

Генератор	Кількість тестів, в яких значення ймовірності $P \le 0{,}01$	Кількість тестів, в яких значення ймовірності $P \le 0{,}001$
BBS	0	0
ДГВБ на основі спарювання точок еліптичних кривих та гешування	1	0

Таблиця 9

Модифікований ДГВБ на основі спарювання точок еліптичних кривих без хешування



Таблиця 10

Модифікований ДГВБ на основі спарювання точок еліптичних кривих та генератор BBS

Генератор	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
Модифікований ДГВБ на основі спарювання точок еліптичних кривих	128 (67,7%)	183 (96,8%)

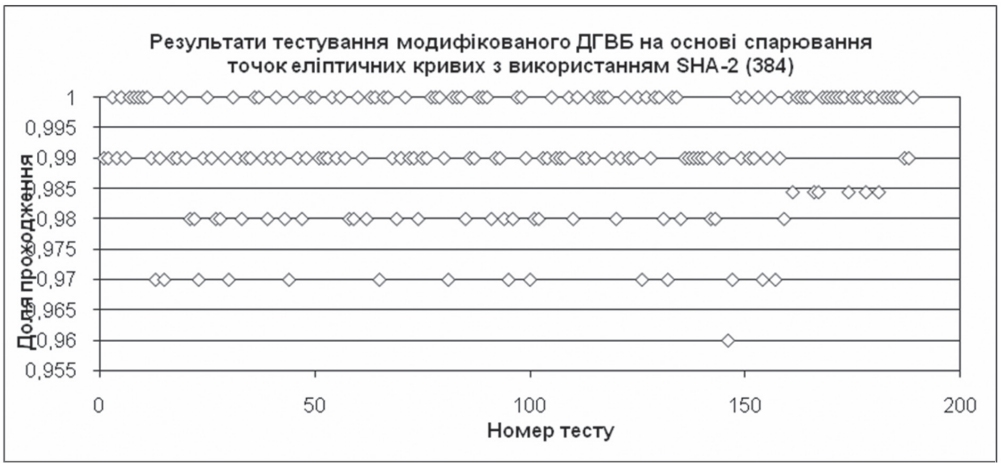
Таблиця 11

Модифікований ДГВБ на основі спарювання точок еліптичних кривих та генератор BBS з урахуванням двох значень P ($P \le 0{,}01$, $P \le 0{,}001$)

Генератор	Кількість тестів, в яких значення ймовірності $P \le 0{,}01$	Кількість тестів, в яких значення ймовірності $P \le 0{,}001$
BBS	0	0
Модифікований ДГВБ на основі спарювання точок еліптичних кривих	7	4

Таблиця 12

Модифікований ДГВБ на основі спарювання точок еліптичних кривих з використанням SHA-2 (384)



Таблиця 13

Модифікований ДГВБ на основі спарювання точок еліптичних кривих з використанням SHA-2 (384) та генератор BBS

Генератор	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
Модифікований ДГВБ на основі спарювання точок еліптичних кривих *SHA-2 (384)*	142 (75,1%)	189 (100%)

Таблиця 14

Модифікований ДГВБ на основі спарювання точок еліптичних кривих з використанням SHA-2 (384) та генератор BBS з урахуванням P ($P \le 0{,}01$, $P \le 0{,}001$)

Генератор	Кількість тестів, в яких значення ймовірності $P \le 0{,}01$	Кількість тестів, в яких значення ймовірності $P \le 0{,}001$
BBS	0	0
Модифікований ДГВБ на основі спарювання точок еліптичних кривих *SHA-2* (384)	1	0

ВИСНОВКИ

Результати експериментальних досліджень підтвердили, що ДГВБ на основі спарювання точок еліптичних кривих та гешування забезпечують формування випадкових детермінованих бітів з достатніми для більшості додатків якостями.

Кращі статистичні характеристики по NIST-SP 800-22 забезпечує модифікований ДГВБ, коли спарювання виконується тільки при обчисленні генератора підгрупи та гешування з використанням функції гешування SHA-2(з довжиною геш значення 384 бітів) по NIST-SP 800 -22.

Як слідує із таблиць 6-8 та 12-14 ДГВБ зі спарюванням точок еліптичних кривих та подальшим гешуванням елементів мультиплікативної підгрупи a_i по статистичним характеристикам перевершують класичний ДГВБ BBS.

Разом з тим для практичної реалізації ДГВБ необхідно ще вирішувати ряд теоретичних та практичних питань. До них необхідно віднести питання генерування загальних параметрів, вибору функцій гешування та їх параметрів, оптимізації обчислень та доведення криптографічних властивостей такого ДГВБ.

Література.

[1] NIST SP 800-90. Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006.

[2] ISO/IEC 18031:2005(E), Information technology – Security techniques – Random bit generation.

[3] *Горбенко І.Д.* Навчальний посібник "Захист інформації в інформаційно-телекомунікаційних системах" / І.Д. Горбенко, Т.О. Гріненко. – Х.: ХНУРЕ, 2003. - 368 с.

[4] *Горбенко І.Д.* Обгрунтування вимог до генераторів випадкових бітів згідно ISO/IEC 18031 / І.Д. Горбенко, Н.В. Шапочка, О.О. Козулін. – К.: Радіоелектронні і комп'ютерні системи, 2009.

[5] *Koblitz N.* Pairing-based cryptography at high security levels, Proceedings of the Tenth IMA International Conference on Cryptography and Coding. / Koblitz N., Menezes A. J. // Springer-Verlag, LNCS 3796. – 2005. –Pp. 13-36.

[6] *Maas M.* Pairing-Based Cryptography / M. Maas. – TECHNISCHE UNIVERSITEIT EINDHOVEN, 2004. – 91p.

[7] *Потій О.В.* Метод оцінки ймовірностей колізій у безумовно стійких та обчислювально стійких криптосистемах / О.В. Потій, Ю.І. Горбенко, Є.В. Попович. // Прикладна радіоелектроніка, 2003.

[8] *Потий О.В.* Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS / А.В. Потий, С.Ю. Орлова, Т.А. Гриненко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вип. 2. С. 206-214.

Надійшла до редколегії 10.06.2010.

Горбенко Іван Дмитрович, доктор техн. наук, професор, завідувач кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, головний конструктор ЗАТ «Інститут інформаційних технологій». Область наукових інтересів: криптографічні системи та протоколи; проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

Шапочка Наталя Вікторівна, аспірантка кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Область наукових інтересів: розробка та застосування методів генерації випадкових послідовностей.

Погребняк Костянтин Анатолійович, канд. техн. наук, асистент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Область наукових інтересів: застосування алгебраїчної геометрії у системах криптографічного захисту інформації; асиметрична криптографія.

УДК 681.324.067

Метод построения детерминированных случайных последовательностей на основе спаривания точек эллиптических кривых / И.Д Горбенко, Н.В. Шапочка, К.А. Погребняк // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 386-393.

Приводится обоснование и описывается сущность и свойства генератора детерминированных случайных последовательностей на основе криптографического преобразования, такого как спаривание точек эллиптических кривых.

Ключевые слова: элиптические кривые, детерминированные случайные последовательности.

Табл. 14. Ил. 01. Библиогр.: 08 назв.

UDK 681.324.067

A method of constructing deterministic random sequences on the base of pairing points of elliptic curves / I.D. Gorbenko, N.V. Shapochka, K.A. Pogrebnyak // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 386-393.

The paper provides substantiation and describes the nature and properties of a generator of deterministic random sequences on the base of cryptographic transformation such as pairing points of elliptic curves.

Key words: elliptic curves, deterministic random sequences.

Tab. 14. Fig. 01. Ref.: 08 items.

УДК 681.3.06

РЕЗУЛЬТАТИ АНАЛІЗУ КРИПТОСИСТЕМ НА ІДЕНТИФІКАТОРАХ, АНАЛІЗ ДОКУМЕНТІВ IEEE P1636.3, RFC 5091, RFC 5408

М.Ф. БОНДАРЕНКО, П.О. КРАВЧЕНКО, Л.В. МАКУТОНІНА

У даній статті представлений загальний опис та характеристика документів криптографічних систем на ідентифікаторах, таких, як RFC 5091, RFC 5408 та IEEE P1636.3™/D1 в області форматів даних і загальної інфраструктури передачі даних в IBE системах. У документі RFC 5408 наводиться архітектура безпеки, необхідні структури даних для криптосистем на ідентифікаторах. Документи RFC 5091 і IEEE P1636.3™/D1 описують системи відкритого ключа на ідентифікаторах, засновані на білінійних спарюваннях.

Ключові слова: інфраструктура відкритих ключів, криптосистеми на ідентифікатори.

ВСТУП

Підтримка інфраструктури відкритих ключів PKI (Public Key Infrastructure) є дуже складним завданням. Зараз надійність багатьох запропонованих систем шифрування з відкритим ключем багато в чому залежить від сертифікату відкритого ключа. Але використання сертифікатів породжує ряд труднощів: проблема анулювання сертифікатів до закінчення терміну дії, передача великої кількості інформації, юридичні складнощі, великі грошові витрати. Проблему PKI можуть розв'язати криптосистеми на основі ідентифікаційних даних.

Спочатку схема шифрування на основі ідентифікаційних даних була запропонована в 1984 році Шаміром з метою спростити сертифікаційну систему. При використанні шифрування на основі ідентифікаційних даних користувачам не треба обмінюватися своїми відкритими ключами. Відкритий ключ користувача легко обчислюється з ідентифікаційних даних користувача. Тільки на етапі розшифрування потрібні послуги центру генерації ключів (Private Key Generator PKG) для того, щоб згенерувати системні параметри і секретний ключ користувача. PKG, використовуючи ідентифікаційні дані, які загальновідомі і представлені в стандартизованому вигляді, обчислює секретний ключ і передає його користувачеві. Хоча така схема породжує деякі складнощі: PKG знає секретні ключі, що в деяких застосуваннях може бути серйозною проблемою; для отримання секретного ключа користувачеві потрібно автентифікацію у PKG; для передачі секретного ключа від PKG користувачеві потрібний захищений канал.

З моменту появи цієї ідеї в 1984 році до недавнього часу побудова схеми зашифрування на основі ідентифікаційних даних залишалася відкритою проблемою. Ситуація змінилася в 2001 році з появою статті Боне-Франкліна (Boneh, Franklin). Боне і Франклін представили схему шифрування на основі ідентифікаційних даних, що використовує властивості білінійних перетворень на еліптичних кривих, яка стала першою повністю функціональною схемою шифрування на основі ідентифікаційних даних.

Раніше білінійні спарювання, а саме спарювання Вейля і спарювання Тейта, використовувалися в криптографії для реалізації MOV атак та FR атак відповідно. Ці атаки засновані на зведенні задачі дискретного логарифмування на еліптичних кривих до задачі дискретного логарифмування в кінцевому полі. Тільки після появи статті Боне-Франкліна білінійні спарювання стали використовуватися не в цілях криптографічного аналізу, а для побудови нових криптографічних протоколів.

Розробка криптографічних систем, заснованих на ідентифікаційних даних та білінійних спарюваннях, є дуже перспективною. З кожним роком росте кількість таких протоколів, що представляються на міжнародних конференціях. Зокрема діє робоча група IEEE P1363.3: Identity-Based Public Key Cryptography, очолювана William Whyte, Terence Spies, що займається розробкою стандарту криптографії на основі ідентифікаційних даних,що використовує білінійні спарювання.

Метою цієї статті є визначення стану стандартизації криптографічних систем на ідентифікаторах та аналіз з наступної розробкою рекомендацій відносно їх застосування.

Криптографія, заснована на ідентифікаторах (IBE), є технологією шифрування відкритого ключа, яка дозволяє відкритому ключу бути обчисленим за допомогою ідентифікатора і набору відкритих математичних параметрів. При цьому враховується відповідний секретний ключ, який буде обчислений за допомогою ідентифікатора, ряду відкритих математичних параметрів, і секретного значення – головного ключа всього домену, – майстер ключа. Відкритий ключ IBE може бути обчислений будь-ким, у кого є необхідні відкриті параметри; майстер ключ необхідний, для обчислення секретного ключа сеансу IBE, обчислення можуть бути виконані тільки сервером, якому довіряють, і який має цей секрет.

Характеристика систем IBE, яка відрізняється їх від інших інфраструктур відкритих ключів тим, що відкриті параметри отримуються користувачем один раз, зашифрування можливе без подальшого з'єднання з сервером під час періоду

дії відкритих параметрів. Традиційна ІВК вимагає наявність підключення користувача до мережі (наприклад, для перевірки статусу сертифіката).

Для реалізації ІВЕ-протоколу обміну повідомленнями необхідні наступні компоненти системи:

1) PKG – Private-key Generator – генератор секретного ключа. PKG містить майстер ключ, який використовується для генерації секретних ключів сеансу ІВЕ. PKG приймає запит користувача на секретний ключ, проводить автентифікацію користувача, і якщо автентифікація пройшла успішно, повертає секретний ключ сеансу ІВЕ.

2) PPS – Public Parameter Server – сервер відкритих параметрів. ІВЕ відкриті параметри включають криптографічні параметри, до яких забезпечений відкритий доступ. Розподіляє, із забезпеченням безпеки, відкриті параметри та інформацію про користувачів системи для PKG.

Схема взаємодії основних елементів ІВЕ-систем представлена на рис.

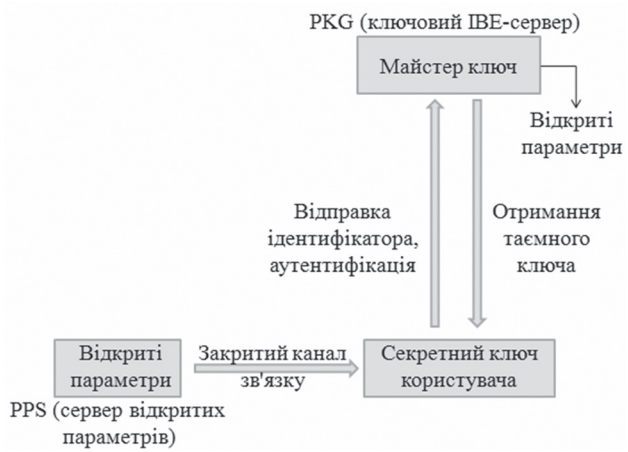


Схема взаємодії базових елементів ІВЕ-систем

1. ВІДПРАВЛЕННЯ ТА ОДЕРЖАННЯ ІВЕ-ЗАШИФРОВАНОГО ПОВІДОМЛЕННЯ

У документах RFC 5408 [1] і RFC 5091 [2], для відправки ІВЕ-зашифрованого повідомлення користувач повинен виконати наступні кроки:

1) Отримати відкриті параметри. Як тільки користувач отримав відкриті параметри, він може виконати операцію зашифрування ІВЕ. Відкриті параметри можуть бути доступними на PPS. URI або IRI, з якого користувачі отримують ІВЕ відкриті параметри повинні бути перевірені на достовірність. У всіх розглянутих документах механізми автентифікації не наводяться, дана тема потребує подальшого опрацьовування і аналізу.

2) Створити і послати ІВЕ-зашифроване повідомлення. Для того щоб зашифрувати повідомлення відправник обчислює сеансовий ключ шифрування, далі – CEK (content-encryption key), та використовує його для зашифрування повідомлення, потім зашифровує CEK на відкритому ІВЕ ключі одержувача. Окрім відкритих параметрів, також необхідний ідентифікатор одержувача, форма якого визначена відкритими параметрами. Коли даний ідентифікатор співпадає з ідентифікатором повідомлення, посланого до цього, тоді не потрібна ніяка додаткова інформація від користувача для відправки зашифрованого повідомлення, яка знадобилася б для відправки незашифрованого повідомлення, і це є однією з переваг систем, заснованих на ІВЕ.

Щоб прочитати ІВЕ-зашифроване повідомлення, одержувач такого повідомлення аналізує його на наявність URI, потім отримує відкриті параметри ІВЕ.

У документах RFC 5408 [1] та RFC 5091 [2], для отримання ІВЕ-зашифрованого повідомлення користувач повинен виконати наступні кроки:

1) отримати відкриті параметри, які дозволяють унікально створити відкриті і секретні ключі. Відкриті параметри надаються сервером PPS по безпечному протоколу. Користувач повинен перевірити, що відповідне ім'я в свідоцтві сервера відповідає URI PPS;

2) отримати секретний ключ ІВЕ. Окрім ІВЕ відкритих параметрів, одержувач повинен отримати секретний ключ, відповідний відкритому ключу, який використовував відправник. Одержувач ІВЕ-зашифрованого повідомлення надає PKG відкритий ключ ІВЕ, який використовується для зашифрування повідомлення і автентифікації повідомлення, і робить запит на секретний ключ, який відповідає відкритому ключу ІВЕ. Секретний ключ надаються PKG по безпечному протоколу;

3) розшифрувати ІВЕ-зашифроване повідомлення. Після отримання необхідного секретного ключа ІВЕ, одержувач використовує цей секретний ключ ІВЕ і передані відкриті параметри ІВЕ для розшифрування CEK.

Далі одержувач використовує CEK, для розшифрування зашифрованого змісту повідомлення.

2. АНАЛІЗ КРИПТОСИСТЕМ НА ІДЕНТИФІКАТОРАХ

Криптосистеми ІВЕ формують таку основу для безпечного середовища обміну повідомленнями, яка відокремлює автентифікацію від шифрування, а також підтримує широкий діапазон джерел автентифікації, для забезпечення ідентифікації користувачів. Розділення автентифікації та шифрування – вкрай необхідна перевага, оскільки дана властивість ІВЕ систем дає можливість організаціям використовувати існуючі механізми (наприклад, каталоги, портали), для підтвердження достовірності користувачів. Дана властивість також дає можливість організаціям використовувати різні ідентифікаційні резерви, для автентифікації різних типів користувачів як відповідних. Далі, можливо, по потребі динамічно коректувати використовуваний механізм автентифікації; наприклад, якщо стосунки з користувачем стають формальнішими, користувач може перейти з використовуваного механізму автентифікації на надійніший механізм автентифікації.

Оскільки секретні ключі в системах ІВЕ генеруються за запитом, відновлення ключа в системах

IBE є тривіальне. Дана можливість дуже спрощує адміністративне розшифрування даних і допускає просту інтеграцію з граничними службами.

Переваги IBE:

1. Забезпечує просту, зручну у використанні процедуру шифрування (відправники потребують лише ідентифікатор одержувача).

2. Дані криптосистеми не вимагають призначеної для користувача попередньої реєстрації для відправників або одержувачів.

3. Підтримка гнучких механізмів автентифікації (не потрібне використання сертифікатів для автентифікації і підпису).

4. Можливий обмін повідомленнями між користувачами з сертифікатами і користувачами, що не мають сертифікатів.

5. Забезпечує автоматичне відновлення ключа.

6. Легка інтеграція з граничними службами передачі повідомлень (службами антиспаму, антивірусного захисту, архівації).

7. Підтримка роботи «off-line» (відправники не потребують перевірки будь-якого з ресурсів, наприклад CRLs або OCSP).

8. Невисока складність обчислень.

По запиту мережевого сканера антивірусу, антиспаму, або іншої прикладки безпеки системи (наприклад, при обміні політиками повідомленнями), можлива генерація сервером PKG на льоту необхідного секретного ключа, для перегляду вмісту повідомлення даних прикладок. Без здатності генерувати і відновити ключі зашифрування за запитом, секретні ключі користувачів мають зберігатися у спеціальному сховищі, потребують надійного захисту, вони мають бути заархівовані, для можливості роботи прикладок з текстом зашифрованих повідомлень.

На відміну від звичайної інфраструктури відкритих ключів, системи IBE не вимагають складної перевірки, попередньої реєстрації або відкликання сертифікатів. Ще одна перевага систем IBE перед системами PKI, – відсутність відкликаних списків сертифікатів та інших списків сертифікатів. Немає по суті жодної потреби в сертифікатах. Замість цього відкритий ключ користувача генерується з його ідентифікатора. Система IBE не вимагає, щоб уповноважений на сертифікацію виробив, засвідчив, або зберіг індивідуальні відкриті ключі.

Єдина інформація, яку надовго зберігає сервер PKG IBE, є «майстер ключ» – по суті велике випадкове число, яке використовується для генерації ключів сеансу користувачів і системних параметрів сервера.

Одна з найважчих проблем для системи PKI, – відкликання сертифікатів, якщо секретний ключ, на якому підписаний сертифікат скомпрометований, або якщо сертифікат потрібно заблокувати. У документі RFC 5408, який описує формати даних IBE-систем, дана проблема вирішується досить просто – в структурі «IBESysParams» (структура, що містить відкриті параметри) включені поле «validity», в якому вказаний період дії відкритих параметрів. Після виділення даного періоду відкриті параметри, а, отже, і відкриті і секретні ключі генеруються заново. Період дії може бути заданий адміністратором безпеки.

Стійкість алгоритмів IBE базується на розв'язанні задачі дискретного логарифму, а також на рішенні задачі білінійної проблеми Диффі-Гелмана.

Переваги IBE протоколів очевидні: такі протоколи роблять непотрібною інфраструктуру відкритих ключів. Замість неї необхідно підтримувати PKG, що значно простіше. Зокрема, якщо всі клієнти використовують один і той же PKG, то вони можуть безпечно спілкуватися і при цьому їм не потрібно шукати відкриті ключі в мережі.

Проте IBE системи мають ряд недоліків:

1. PKG знає секретний ключ одержувача, що в деяких застосуваннях може бути серйозною проблемою. Цей недолік можливо усунути, якщо застосовувати схеми розподілу таємниці, наприклад, зберігати майстер ключ по частинам на різних серверах PKG.

2. PKG повинен провести автентифікацію користувача (як і в системах з Центрами сертифікації).

3. Для передачі секретного ключа від PKG до користувача, що його отримує, необхідний захищений канал.

4. Одержувач публікує свої PKG відкриті параметри і відправнику необхідно отримати ці параметри, перш ніж відправляти одержувачу зашифрований лист.

Описані схеми шифрування дозволяють значно знизити загальну складність протоколів обміну ключами.

3. СТАНДАРТИЗАЦІЯ КРИПТОГРАФІЧНИХ СИСТЕМ НА ІДЕНТИФІКАТОРАХ

Керівним стандартом в галузі криптографічних систем на ідентифікаторах є проект стандарту IEEE P1363.3 [7] – Draft Standard for Identity-based Public-key Cryptography Using Pairings – Проект стандарту для криптографічних систем з відкритим ключем, заснованих на ідентифікаторах, що використовує спарювання. Проект стандарту 2008 року IEEE P1363.3 – стандарт, призначений для локальних мереж 802.1 – 802.12, розроблений робочими групами проекту 802 Інституту Інженерів по Електротехніці та Радіоелектроніки (IEEE).

Також, технічними специфікаціями, для реалізації схем криптографічних систем на ідентифікаторах є документи RFC 5408-2009 та RFC 5091-2007.

RFC 5408 – Identity-Based Encryption Architecture and Supporting Data Structures – Архітектура та підтримуючі структури даних, для криптографічних систем на ідентифікаторах. Документ RFC 5408-2009 [1] описує архітектуру безпеки, потрібну для здійснення шифрування, заснованого на ідентифікаторах. Описує протокол шифрування ключа, що використовує ідентифікатор, як відкритий ключ. Визначає структури даних, які

можуть бути використані, для здійснення такого протокола.

RFC 5091 [2] – Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems – Стандарт криптографічних систем на ідентифікаторах: Реалізація схем BF та BB1 на суперсингулярній еліптичній кривій. Документ RFC 5091 надає набір специфікацій для реалізації IBE систем шифрування, заснованих на білінійних спарюваннях. Описані дві криптосистеми: система IBE, запропонована Boneh і Franklin (BF), і система IBE, запропонована Boneh і Boyen (BB1). Приведені безпечні і практичні виконання для кожної системи, що охоплюють основні алгоритми IBE, з рівнем безпечності, що зазвичай досягається у гібридних схемах.

4. КОРОТКИЙ ОПИС IBE СХЕМ, ПРИВЕДЕНИХ У ДОКУМЕНТІ RFC 5091-2007

Обчислення і відкритих, і секретних ключів в системі IBE відносно RFC 5091-2007 може відбуватися за потребою, і є результатом своєчасного створення і відкритих, і секретних ключів. Це контрастує з іншими криптосистемами на відкритих ключах, в яких ключі генеруються псевдовипадково і розподіляються перед встановленням відкритого з'єднання, і в яких секретні ключі розшифрування повинні бути надійно архівовані, щоб можна було скористатися їх копіями, у випадку, якщо вони втрачені або зруйновані. Здатність обчислити одержувачем відкритий ключ зокрема позбавляє від необхідності відправника і одержувача взаємодіяти один з одним, або безпосередньо, або через проксі-сервер, такий як директивний сервер, перш ніж послати безпечні повідомлення.

Криптографічна система Boneh-Franklin (BF)

Криптографічна система BF в документі RFC 5091-2007 основана на шифруванні в групі точок еліптичної кривої, та складається з трьох наступних алгоритмів:

• алгоритм BFsetup – виробляє майстер ключ і генерує відкриті параметри; має дві версії Bfsetup і Bfsetup1, обидві версії випадково вибирають майстер ключ і зв'язані відкриті параметри; результуючий майстер ключ і відкриті параметри окремо зашифровуються;

• алгоритм BFderivePubl – утворює відкритий ключ з ідентифікатора користувача і дійсних відкритих параметрів, за допомогою приведених нижче геш-функцій у вигляді точки ЄК;

• алгоритм BFextractPriv – утворює секретний ключ сеансу з ряду дійсних відкритих параметрів і відповідного майстер ключа, результат роботи алгоритму – точка ЕК.

Криптографічна система Boneh-Boyen (BB1)

Криптографічна система BB1 в документі RFC 5091-2007 також основана на шифруванні в групі точок еліптичної кривої, та складається з трьох наступних алгоритмів:

• алгоритм BBsetup – виробляє майстер ключ і генерує відкриті параметри; випадково вибирається набір головних ключів і зв'язаних відкритих параметрів. Вхід і вихід алгоритму аналогічний BF;

• алгоритм BBderivePubl – утворює відкритий ключ з ідентифікатора користувача і дійсних відкритих параметрів, за допомогою приведених нижче геш-функцій у вигляді цілого числа;

• алгоритм BBextractPriv – утворює секретний ключ сеансу з ідентифікатора, ряду дійсних відкритих параметрів і відповідного майстер ключа, вихід алгоритму – дві точки ЄК.

Геш-функції та параметри безпечності, наведені в RFC 5091-2007.

Параметр *n* відповідає довжині модуля в бітах, як і у класичних криптографічних системах відкритого ключа типу Діфі-Гелмана або RSA.

Таблиця 1

Визначення залежних параметрів безпеки *n_p*, *n_q* і відповідних геш-функцій

n	*n_p*	*n_q*	*hashfcn*
1024	512	160	SHA-1
2048	1024	224	SHA-224
3072	1536	256	SHA-256
7680	3840	384	SHA-384
15360	7680	512	SHA-512

5. КОРОТКИЙ ОПИС І АНАЛІЗ ФОРМАТІВ ДАНИХ СИСТЕМИ IBE ЗАПРОПОНОВАНИХ В RFC 5408

У RFC 5408 визначається, як саме відновлюються відкриті параметри у системах IBE. Клієнт, під час передачі або отримання, повинен виконувати конфігурацію цих параметрів вручну, наприклад, через редагування файлу конфігурації. Для спрощення конфігурації, клієнт повинен також надіслати запит відкритого параметра URI/IRI [5,6], що описаний в RFC 5408, для вибору відкритих параметрів, заснованих на конфігурації URI/IRI. Це особливо корисно для інтеграції між системами IBE. Ці відкриті параметри можуть використовуватися, для розшифрування повідомлення одержувачами, вони засвідчують особу і відновлюють секретні ключі даного PKG.

Усі структури і типи даних зберігаються в об'єднаному модулі ASN.1.

Структура IBEIdentityInfo використовується для передачі ідентифікатора одержувача (є зашифрованою).

Структура uriPPSOID містить поля, що заповнюються одержувачем або відправником, містить відкриті параметри.

Структура IBESysParams містить відкриті параметри IBE. IBEPublicParameters – структура, що містить відкриті параметри, відповідні алгоритмам IBE, які підтримують PKG.

Відповідно до документу RFC 5408 у стандартному реєстраційному дереві повинні реєструватися три типи носіїв:

• The application/ibe-pp-data MIME type – тип носія, який передає відкриті параметри, необхідні для операцій криптографічної системи;

• The application/ibe-key-request+xml MIME type – тип носія, який містить рекомендації по автентифікації, клієнт може використовувати ці рекомендації, для формування запиту ключа, який містить додаткові дані автентифікації;

• The application/ibe-pkg-reply+xml MIME type – тип носія, за допомогою якого по захищеному протоколу передається секретний ключ IBE. Перед передачею користувач перевіряє свідоцтво сервера.

Формат відповіді сервера PKG.

У документі RFC 5408 визначені наступні формати відповіді сервера PKG:

IBE100 KEY_FOLLOWS – містить структуру IBEPrivateKeyReply. При правильному запиті повертає секретний ключ – структуру privateKey.

IBE101 RESERVED – поле, що відповідає за функціональну сумісність нових версій протоколу. Якщо в ньому міститься інформація, то користувач повинен відмовитися від отриманих даних.

IBE201 FOLLOW_ENROLL_URI – містить елемент <ibe:location>, який визначає механізм автентифікації URI, містить сертифікат автентифікації, який надалі використовує користувач в елементі запиту ключа <ibe:authData>.

IBE300 SYSTEM_ERROR – вказує на внутрішню помилку сервера.

IBE301 INVALID_REQUEST – містить інформацію, яка може допомогти діагностувати помилку.

IBE303 CLIENT_OBSOLETE – даний код відповіді вказує, що сервер нездібний правильно обробити запит, оскільки версія запиту вже не підтримується сервером.

IBE304 AUTHORIZATION DENIED – даний код відповіді вказує, що сервер отримав ключовий запит, але сертифікат автентифікації був заблокований.

Якщо користувач отримав IBE300, IBE301, IBE303, чи IBE304 код відповіді, він повинен перервати запит ключа і відмовитися від будь-яких даних, включених в тіло відповіді.

6. КОРОТКИЙ ОПИС ТА АНАЛІЗ ПРОЕКТУ СТАНДАРТУ IEEE P1636.3-2008

Стандарт визначає загальні криптографічні методи з відкритим ключем, засновані на ідентифікаторах, які використовують спарювання, включаючи математичні примітиви секретних ключів, шифрування на відкритому ключі, цифрові підписи, і схеми шифрування, засновані на цих примітивах [7]. Даний стандарт також визначає алгоритми використовуваних геш-функцій, зв'язані параметри шифрування, відкриті ключі і секретні ключі.

Стандарт P1363-3 приводить довідкову інформацію для специфікацій різноманітних протоколів на спарюваннях, з яких прикладки можуть вибрати і цей стандарт визначає структуру цих методик, яка дозволяє вибрати відповідну методику, для певної прикладки. Криптографія, заснована на спарюваннях, допускає інші компактніші версії традиційних криптографічних методів, такі як короткі схеми підписів, або методики управління ключами, які можуть відобразити вибраний із прикладки ідентифікатор у відкритий ключ.

Структура криптографічних методик, заснованих на спарюваннях, подібна визначеній в IEEE 1363a, де важко здійсненна теоретико-числова задача використовуються як підстава для криптографічних схем, які включені в протоколи. Заснована на спарюваннях криптографія використовується по-різному, але зв'язана з набором завдань, які, імовірно, є, в обчислювальному відношенні, нездійсненними у відповідних розмірах. Ці проблеми, типові варіанти білінійної задачі Diffie-Hellman (BDH), викладеної в 1363a.

Загальна структура примітивів описана в Розділах 5, 6,7 P1363-3; специфікація схем визначена в Розділі 8 P1363-3. Даний стандарт не визначає протоколи, вони є специфічними для кожної окремої прикладки і не розглядаються в даному стандарті. Проте, методики, визначені в цьому стандарті, є ключовими компонентами для створення різних криптографічних протоколів. Крім того, Додаток D стандарту P1363-3 описує, які методики можуть використовуватися в протоколах, для досягнення певних атрибутів безпеки.

Примітиви, використані в стандарті P1363-3

Примітиви, визначені в стандарті P1363-3:

• примітиви, засновані на спаровуваннях Діфі-Гелмана, у рандомізованих і нерандомізованих формулюваннях;

• примітиви, засновані на сліпих комутативних спаровуваннях;

• примітиви, засновані на спаровуваннях геш-функції параметрів домену.

У кожного з цих примітивних типів є чотири складові:

• генерація;

• перевірка згенерованого значення;

• зашифрування;

• розшифрування.

Примітиви в цьому стандарті представляються як математичні операції, і використовуються як стандартні блоки для повних схем. Виконання примітивного підпису може повернути щось схоже на підпис, навіть якщо на його вході не було дійсного секретного ключа, або ж виконання може також відхилити вхідні дані. Користувач примітиву повинен дати гарантію того, що вхідні значення задовольняють обмеженням або повинен включати релевантні перевірки. Наприклад, користувач може використовувати релевантний ключ і методи ратифікації параметра домену.

Специфікація примітиву складається з наступної інформації:

• вхід до примітиву;

• припущення про вхід, приведені в описі операції, виступаючої примітивом;

• вихід примітиву;

• операція, виконана примітивом, виражена рядом кроків;

• рекомендації області відповідності, що описують мінімальний набір входів, для яких виконання повинне проходити відповідно до примітиву, що рекомендується (див. Додаток В P1363-3).

Формат входів, виходів і процедури виконання примітивів, не розглядаються у цьому стандарті. Див. Додаток Е P1363-3 для отримання додаткової інформації про формати входу і виходу.

Схеми, запропоновані стандартом P1363-3

Типи схем, визначені стандартом P1363-3:

• шифрування, засноване на ідентифікаторах;

• інкапсуляція ключа, заснована на ідентифікаторах;

• підписи, засновані на ідентифікаторах.

Мета цих схем полягає в створенні захищеного каналу зв'язку між декількома сторонами, з імовірно присутніми, одним або декількома уповноваженими на генерацію. Дані схеми дозволяють відправнику перетворювати ідентифікатор одержувача, ряд ключових параметрів сервера, у відкритий ключ. Відкритий ключ може використовуватися для шифрування або отримання симетричного ключа. Одержувач повинен потім зробити запит на секретний ключ від уповноваженого на генерацію.

Схеми в даному стандарті представляються в загальній формі, заснованій на певних примітивах і додаткових методах шифрування повідомлення. Схеми також включають операції управлінням ключа, такі як вибір секретного ключа або отримання відкритого ключа іншої сторони. Для належної безпеки сторона повинна бути упевнена в цілісності та справжності ключа власника та відкритих параметрів.

У специфікацію схеми входить наступна інформація:

• опції схеми, такі як альтернативи для примітивів і додаткові методи;

• одна або більш операцій, залежно від схеми, виражені у ряді кроків;

• рекомендації області відповідності для реалізації відповідної схеми (див. Додаток В [7]).

Протоколи, наведені у проекті стандарту P1363.3

У IEEE P1363.3 наведені два криптографічних примітиви, які по своєї суті є протоколами встановлення ключа, це два протоколи встановлення ключа, що засновані на спарюваннях – схема Ванга та схема SCK (Smart-Chen-Kudla).

Дані протоколи дозволяють встановити відкриті та секретні ключі користувачам, для подальшого використання цих ключових даних в схемах шифрування повідомлень.

Опис геш-функцій, які використовуються в IEEE P1636.3

Стандартом IEEE P1636.3 рекомендовано до застосування три типа геш-функцій:

• геш-функція до цілого числа – IHF1-SHA;

• геш-функція до рядка – SHF1-SHA;

• геш-функція до точки на кривій – PHF1-SHA.

Функція IHF1-SHA використовує сім'ю SHA-1 та SHA-2 геш-функцій, для перетворення рядка до цілого числа. Інші геш-функції можуть бути сконструйовані за потребою за допомогою використання IHF1-SHA.

Таблиця 2

Визначення параметра захисту і відповідної геш-функції

Параметр безпечності, *t*	Використовувана геш-функція, *H*
80	SHA-1
112	SHA-224
128	SHA-256
192	SHA-384
256	SHA-512

ВИСНОВОК

Практичне застосування інфраструктур відкритого ключа на сертифікатах виявила ряд недоліків та проблемних питань. Серед них необхідно виділити значну вартість, психологічну неприйнятність, недостатній рівень уніфікації тощо. Вказані недоліки можуть бути видалені при застосуванні криптосистем на ідентифікаторах. Основоположним принципом таких систем є те, що в якості відритого ключа асиметричної пари, причому незалежно від методу перетворення, використовується відкриті дані користувача, наприклад e-mail, почтова адреса тощо.

В даній роботі підлягали аналізу такі документи, як RFC 5091, RFC 5408, IEEE P1636.3. Загальним у розглянутих документах є застосування алгоритмів Boneh-Franklin и Boneh-Boyen. У документах RFC 5091, RFC 5408, IEEE P1636.3 обов'язковою вимогою є підтвердження достовірності відправника і одержувача повідомлення, генератора секретного ключа і сервера відкритих параметрів. Механізми автентифікації не приводяться в документах RFC 5091, RFC 5408, IEEE P1636.3, проте обов'язкові до застосування.

У документі RFC 5408 приводиться загальний опис алгоритмів Boneh-Franklin і Boneh-Boyen, приведені протоколи обміну інформацією в IBE-схемах, описані використовувані в даних протоколах структури і типи даних.

Документ RFC 5091 використовує математику в групі точок еліптичної кривої. Як відкриті параметри має характеристики кривої, дві точки на EK, номер версії алгоритму.

У проекті стандарту IEEE P1636.3 описані три алгоритми шифрування, засновані ідентифікаторах, що використовують спарювання точок EK – це алгоритми BB1-IBE, BB1-KEM та алгоритм BF-IBE.

В даному стандарті приводиться наступна загальна модель побудови IBE-схем, заснованих на спарюваннях точок EK:

1) Примітиви – базові математичні операції (примітиви, засновані на спарюваннях Діфі-Гелмана; примітиви, засновані на сліпих комутативних спарюваннях и т. п.).

2) Схеми – зв'язані операції, що комбінують примітиви та додаткові методи (шифрування, інкапсуляція ключа та підписи, засновані на ідентифікаторах).

3) Протоколи – послідовності операцій, які виконуються декількома сторонами, для досягнення деякого заданого рівня безпечності.

З погляду застосування, примітиви можуть бути реалізовані на нижньому рівні (наприклад, реалізовані в межах апаратних або програмних модулів), схеми можуть бути реалізовані на середньому рівні (наприклад, реалізовані в межах криптографічних бібліотек сервісу), і протоколи можуть бути розглянуті як реалізація вищого рівня (наприклад, реалізовані в межах повних наборів застосувань).

Проект стандарту P1636.3™/D1-2008, на відміну від документу RFC 5091-2007, в якому використовується одна функція гешування SHA, може використовуватися декілька функцій гешування. В алгоритмі BB1-KEM використовується дві функції гешування – IHF-SHA і SHF-SHA. Алгоритм BB1-IBE аналогічний алгоритму BB1-KEM, основна відмінність – використовується три функції гешування – дві IHF1-SHA і SHF1-SHA.

Відкритий ключ у всіх алгоритмах розглянутих документах обчислюється за допомогою функції гешування від ідентифікатора і відкритих параметрів.

Проведені дослідження та порівняльний аналіз показали, що описані документи дозволяють реалізувати криптоперетворення на ідентифікаторах, забезпечують необхідний рівень стійкості у випадку застосування перетворень на еліптичній кривій. Запропоновані функції гешування є стійкими до визначення прообразу, другого прообразу, а також є стійкими до колізій. При використанні алгоритмів, що визначені в стандартах забезпечується необхідний рівень таких послуг, як конфіденційність та неспростовність. Розглянуті документи можуть бути гармонізовані в Україні та прийняті у якості технічних специфікацій.

Література.

1. *Martin, M. Schertler, G. Appenzeller,* "Identity-Based Encryption Architecture and Supporting Data Structures", RFC 5408, January 2009.
2. *X. Boyen, L. Martin,* "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", RFC 5091, December 2007.
3. *D. Boneh and M. Franklin,* "Identity-based encryption from the Weil pairing," in Proc. of CRYPTO 01, LNCS 2139, pp. 213-229, 2001.
4. *D. Boneh and X. Boyen,* "Efficient selective-ID secure identity based encryption without random oracles," In Proc. of EUROCRYPT 04, LNCS 3027, pp. 223-238, 2004.
5. *Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee,* "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.
6. *Duerst, M. and M. Suignard,* "Internationalized Resource Identifiers (IRIs)", RFC 3987, January 2005.
7. *Hoes Lane,* "Draft Standard for Identity-based Public-key Cryptography Using Pairings", IEEE P1636.3™/D1, April 2008.

Надійшла до редколегії 15.06.2010.

Бондаренко Михайло Федорович, член-кореспондент НАН України, Лауреат державної премії України, доктор технічних наук, професор, ректор Харківського національного университету радіоелектроніки.

Макутоніна Лідія Вікторівна, студент групи ІБ-06-2 ХНУРЕ. Область наукових інтересів: асиметричні криптосистеми, криптографічні системи на ідентифікаторах.

Кравченко Павло Олександрович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: асиметричні криптосистеми, криптографічні системи на ідентифікаторах.

УДК 681.3.06

Результаты анализа криптосистем на идентификаторах, анализ документов IEEE P1636.3, RFC 5091, RFC 5408/ М.Ф. Бондаренко, П.О.Кравченко, Л.В. Макутонина // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 394–400.

Приведены результаты классификации и сравнительного анализа криптографических систем на идентификаторах, а также краткое описание основных стандартов криптографических систем на идентификаторах, которые рекомендуется принять в Украине в виде технических спецификаций.

Ключевые слова: инфраструктура открытых ключей, криптосистемы на идентификаторах.

Табл. 2. Ил.1. Библиогр.: 7 назв.

UDC 681.3.06

Results of analyzing the identity-based encryption, analysis of documents IEEE P1636.3, RFC 5091, RFC 5408 / M.F. Bondarenko, P.O. Kravchenko, L.V. Makutonina// Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 394-400.

The results of classification and comparative analysis of identity-based encryption are presented. A brief description of basic standards of the identity-based encryption which are recommended to be accepted in Ukraine as technical specifications, is given.

Key words: PKI, identify-based cryptosystem.

Tab. 2. Fig. 1. Ref.: 7 items.

УДК 681.3.06:519.248.681

ПРОБЛЕМНІ ПИТАННЯ ЕЛЕКТРОННОЇ АВТЕНТИФІКАЦІЇ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

Д.В. ІВАНЕНКО, Є.П. КОЛОВАНОВА

В даній статті викладено результати аналізу основних напрямів здійснення електронної автентифікації та розробка відповідних пропозицій з орієнтацією на роботи в технологічно розвинених державах. Електронна автентифікація може базуватися на застосуванні криптографічних та біометричних методів. За цієї умови забезпечується необхідна якість автентифікації.

Ключові слова: електронна аутентифікація, системи контролю доступу.

В Україні та у всьому світі в цілому в галузі захисту інформації широке впровадження отримують інфраструктури з відкритими ключами. Створення інфраструктури дозволяє вирішити ряд питань: забезпечити надання користувачам базових послуг таких як конфіденційність, цілісність, доступність, але залишаються відкритими та актуальними задачі, що пов'язані з електронною ідентифікацією та автентифікацією суб'єктів та об'єктів. На сьогодні виникає необхідність мати гарантії особи, що звернулася до системи, і забезпечити належний рівень автентифікації, як особи, що сформувала запит до системи, так і сформованої відповіді на електронний запит.

У нинішній час цьому напряму призначається значна увага. У світі вирішенням цієї задачі займаються декілька країн, але кожна з них використовує різні підходи. Метою цієї статті є викладення результатів аналізу основних напрямів здійснення електронної автентифікації та розробка відповідних пропозицій з орієнтацією на роботи в технологічно розвинених державах.

Найвпливовішим поштовхом вирішення цього питання у США можна назвати Президентську Директиву США про внутрішню безпеку (HDSP-12). Очікувалось, що директива змінить становище ринку негайно, але проблеми фінансування проекту та ненадходження відповідного сертифікованого обладнання призвело до зниження темпів впровадження. З часом уряд почав більше приділяти уваги цьому питанню – зріс бюджет, до директиви почали прислухатися комерційні організації, внаслідок, зріс попит та приплив позабюджетних коштів. Основна робота направлена на автентифікацію, управління конфіденційними даними та контроль доступу до даних, синхронізацію облікових записів тощо. Найбільш вагомим результатом є розробка та прийняття федерального стандарту США FIPS 201, який висуває вимоги до електронних даних осіб, життєвих циклів посвідчень тощо.

У Великобританії напрям застосування був більш комерційний, за що набув широкого попиту. Британською асоціацією індустрії безпеки розробляються рекомендації до використання систем контролю доступу на виробництвах. Ці рекомендації розкриватимуть загальні характеристики побудови таких систем, будуть підкреслювати особливі моменти (положення) національного та міжнародного стандартів, що регламентують використання систем контролю доступу.

У РФ значна увага приділяється методам та механізмам автентифікації. Посилаючись на досвід інших країн у розв'язанні задач контролю доступу, зрозуміло, що найактуальнішим питанням є електронна автентифікація особи. Роблячи на цьому акцент, було розроблено та прийнято відповідний стандарт ГОСТ Р 52633-2006 «Требования к средствам высоконадежной биометрической аутентификации».

Можна стверджувати, що всі країни-розробники систем контролю доступу до даних прийшли до висновку, що необхідно приділяти особливу увагу електронній автентифікації. Надійність такої автентифікації можна забезпечити з використанням, наприклад, біометричних характеристик людини. Це насамперед стало можливо завдяки деяким перевагам цієї технології:

• біометричні шаблони важко фальсифікувати;

• в силу унікальності біометричних характеристик достовірність автентифікації за біометричними даними дуже висока;

• біометричний ідентифікатор не можна забути або загубити, як пароль чи картку.

З розвитком технологій розроблені та знаходять використання різні біометричні методи автентифікації. Характеристики найбільш розповсюджених методів автентифікації за біометричними параметрами людини наведені в табл. 1.

Таблиця 1

Біометричні методи

Біометричний метод	FAR (імовірність допуску «іншого»), %	ERR (імовірність відмови від допуску «свого»), %	Час верифікації, с
Геометрія обличчя	0,1	0,1	1
Параметри сітківки ока	0,0001-0,00078	0,4 - 0,00066	1,5 - 4
Відбиток пальця	0,1-0,0001	0,01-3	0,5 – 3
Геометрія руки	0,0001	1	2
Райдужна оболонка	0,01	0,18	-

Проведений аналіз показав, що при розробці кожного з цих методів виникають проблеми: нечіткість відтворення біометричних даних, нерівномірний розподіл біометричної інформації. Також в процесі використання треба враховувати наступні складності:

• при використанні динамічних біометричних даних потрібно враховувати залежність фізичного та емоційного стану особи;

• біометричні дані не є секретними, оскільки люди залишають їх повсюди (наприклад, відбитки пальців).

Наші дослідження показали, що незважаючи на всю різноманітність методів біометрії, самим розповсюдженим залишається такий метод як відбитки пальців (майже 60% ринку біометрії). При виборі оптимального методу акцент робиться на економічні показники (витрати), мобільність (малогабаритність устаткування), стійкість, і проаналізувавши залежність (див. рис. 1) цих показників вибір пав на метод відбитків пальця. Наш вибір автентифікації за відбитком пальців підтверджується вибором США біометричного методу для стандарту (FIPS 201).

Розгортаючи системи контролю доступу потрібно звертати увагу на розмежування доступу для більш якісного захисту. Слушний метод вирішення саме цього питання було запропоновано США та затверджено у стандарті FIPS 201. Насамперед стандарт передбачає введення своїх рівнів гарантії автентифікації особи (табл. 2.):

– довіра базового рівня, коли забезпечується базовий ступінь гарантії справжності (автентичності) особи;

– довіра вищого рівня, коли забезпечується суттєво підвищений ступінь гарантії справжності (автентичності) особи;

– дуже високий рівень, коли забезпечується надвисокий ступінь гарантії справжності (автентичності) особи.

Таблиця 2

Рівні гарантії

Рівні електронної автентифікації		Зіставні PIV Рівні запевнення
Номер Рівня	Опис	
Рівень 2	Деяка довіра до заявленої перевіреної особи	ДЕЯКА довіра
Рівень 3	Висока довіра до заявленої перевіреної особи	ВИСОКА довіра
Рівень 4	Дуже Висока довіра до заявленої перевіреної особи	ДУЖЕ ВИСОКА довіра

FIPS 201 пропонує розмежувати доступ на фізичний та логічний, також до кожного з них він рекомендує свої механізми автентифікації (див. табл.3. та табл.4.). Залежно від рівня гарантії стандарт пропонує різні механізми автентифікації особи, розповімо про кожний з ростом складності:

• VIS – механізм автентифікації, що ґрунтується на використанні візуальних посвідчень, як правило підтримується для управління доступу до фізичних ресурсів та засобів;

• CHUID – механізм автентифікації, що ґрунтується на використанні унікального ідентифікатора утримувача картки, який доступний як з контактних, так і без контактних інтерфейсів;

• Механізм автентифікації з використанням біометричної автентифікації, в залежності від доступу поділяється на два типа:

1. BIO – автентифікація на основі біометричної інформації без контролю зі сторони служби безпеки;

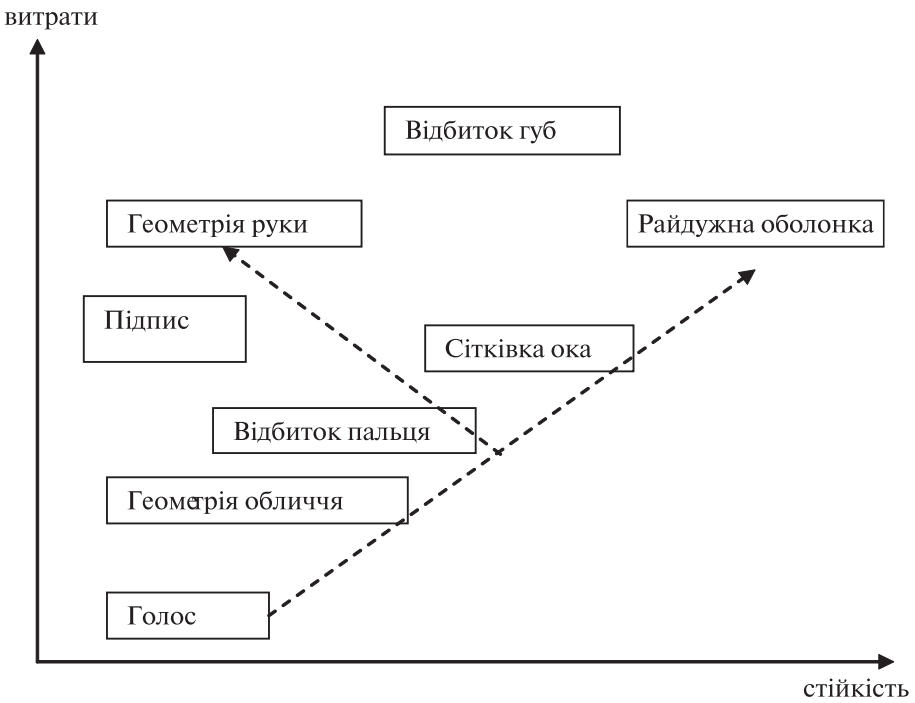


Рис. 1. Залежність вибору біометричного методу від рівня стійкості та витрат на його впровадження

2. BIO-A – автентифікація на основі біометричної автентифікації з контролем зі сторони служби безпеки (наприклад, за ходом автентифікації спостерігає інспектор або адміністратор з безпеки).

• PKI – механізм автентифікації з використанням асиметричних криптографічних перетворень.

Таблиця 3

Логічний доступ

Рівень гарантій	Механізм автентифікації, що застосовується	
	середовище локальної робочої станції	середовище віддаленої мережевої системи
Довіра базового рівня	CHUID	PKI
Довіра вищого рівня	BIO	
Довіра дуже високого рівня	BIO-A, PKI	

Таблиця 4

Фізичний доступ

Рівень гарантій	Механізм автентифікації
Довіра базового рівня	VIS, CHUID
Довіра вищого рівня	BIO
Довіра дуже високого рівня	BIO-A, PKI

Перевагою даної структури є теще механізми автентифікації вищого рівня гарантії можуть бути застосовані до нижчого рівня гарантії, кожен механізм може бути додатково посилений використанням інфраструктурою верифікації стану сертифіката. Таким чином, США була зроблена кропітка робота по розробленню оптимальних рекомендації щодо створення систем контролю доступу, які були направлені на створення своїх рівнів гарантії, та полегшив вибір механізмів ідентифікації та автентифікації при створенні аналогічної системи.

В роботі розглянуто проблемні питання систем контролю доступу при їх розробці та використанні, був досліджений досвід інших країн, які вже використовують систем контролю доступу. Насамперед стало зрозуміло, що значну увагу слід приділяти електронній автентифікації, для чого необхідно врахувати такі фактори, як:

• рівні гарантії;

• доступ;

• механізми автентифікації, відповідно до наведених вище факторів.

З проведеного аналізу можна зробити висновок, що на теперішній час актуального стає автентифікація за біометричними ознаками. Враховуючи такі фактори, як рівень стійкості та витрати на впровадження біометричного методу, найбільш актуальним та перспективним є автентифікція за відбитками пальців.

Література:

[1] FIPS PUB 201.Personal Identity Verification (PIV) of Federal Employees and Contractors. 2006

[2] HDSP-12. Homeland Security Presidential Directive 12.2003

[3] British Security Industry Association. http://www.bsia.co.uk/

[4] ГОСТ Р 52633-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

[5] Биометрическая защита.http://www.securitylab.ru/contest/387619.php

Надійшла до редколегії 18.06.2010.

Іваненко Дмитро Вікторович, аспірант кафедри безпеки інформаційних технологій ХНУРЕ. Область наукових інтересів: інформаційні технології, захист інформації, методи та засоби автентифікації даних.

Колованова Євгенія Павлівна, асистент кафедри безпеки інформаційних технологій ХНУРЕ. Область наукових інтересів: інформаційні технології, захист інформації, методи та засоби автентифікації даних, розпізнавання зображень

УДК 681.3.06:519.248.681

Проблемные задачи электронной аутентификации в системах контроля доступа / Д.В. Иваненко, Е.П. Колованова // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010. Том 9. № 3. – С. 401-403.

В статье изложены результаты анализа основных направлений осуществления электронной аутентификации и разработка соответствующих предложений с ориентацией на применение в технологически развитых государствах. Электронная аутентификация может базироваться на применении криптографических и биометрических методов. При этом условии обеспечивается необходимое качество аутентификации.

Ключевые слова: электронная аутентификация, системы контроля доступа.

Табл. 03. Ил.01. Библиогр.: 05 назв.

UDC 681.3.06:519.248.681

Problem issues of electronic authentication in access control systems / D.V. Ivanenko, I.P. Kolovanova // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 401-403.

The paper presents the results of analyzing the main trends of electronic authentication implementation and development of appropriate proposals oriented on the implementation in technologically developed countries. Electronic authentication can be based on applications of cryptographic and biometric methods. The required quality of authentication is provided under this condition.

Key words: electronic authentication, access control systems.

Tab. 03. Fig. 01. Ref.: 05 items.

УДК 004.056:[336.71(430)+336.71(477)]

ПОРІВНЯЛЬНИЙ АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ НАЦІОНАЛЬНИХ БАНКІВ УКРАЇНИ ТА НІМЕЧЧИНИ

Ю.І. ГОРБЕНКО, І.Ф. АУЛОВ, Є.Ю. КУТЯ, Д.Е. ХРЯПІН

Наводяться результати аналізу та порівняння криптографічних примітивів, що застосовуються та плануються до застосування для захисту інформації в банківських інформаційних технологіях України та Німеччини. Визначено перелік стандартів, що пропонується до впровадження та застосування на території України

Ключові слова: криптографічні системи, криптографічні примітиви.

ВВЕДЕННЯ

Нині в Україні створені та надійно функціонують банківські інформаційні технології та системи. По суті, починаючи з 1992 року в них значна увага приділяється питанням захисту банківської інформації [проект CrypTool, 1], створені та функціонують комплексні системи захисту інформації. Обов'язковими послугами, що повинні надаватись в них клієнтам та власникам, є такі послуги, як неспростовність, цілісність, справжність, доступність, конфіденційність та надійність [ISO 15408]. Якість надання вказаних послуг та рівень гарантій в суттєвій мірі визначається методами (перетвореннями), механізмами та протоколами криптографічного захисту інформації. Також визнано, що для надання вказаних послуг з необхідним рівнем гарантій необхідно використовувати асиметричні та симетричні криптографічні перетворення, а також криптографічні протоколи автентифікації та встановлення ключів, що на них ґрунтуються.

Одним із проблемних питань надійного функціонування банківських інформаційних технологій є забезпечення інтероперабельності, в тому числі в частині криптографічного захисту інформації. Зважаючи на актуальність вказаних задач, в Україні та Германії широко застосовуються міжнародні та національні стандарти, а також рекомендації, що визначають вимоги до систем обробки та захисту інформації [проект CrypTool,1]. Проте, як показав аналіз, в обох державах виникають проблемні питання забезпечення інтероперабельності, як у плинний час, так і з прийняттям нових та оновленням стандартів та рекомендацій, що є необхідним при взаємодії на міжнародному та міждержавному рівнях. Тому, на наш погляд, важливою є задача вивчення та порівняння стану застосування криптографічних перетворень та механізмів, перше за все в частині стандартизації.

Результати попереднього аналізу показали, що в Німеччині зроблені суттєві кроки та отримані певні результати в частині використання методів та протоколів криптографічного захисту інформації [2]. У зв'язку з цим для України важливим є вивчення досвіду Німеччини та визначення можливостей його застосування в частині криптографічного захисту інформації взагалі та у банківській сфері частково.

Що стосується стандартизації, то потрібно відмітити, що значна частина європейських та міжнародних стандартів захисту інформації була досліджена та/або запропонована інститутами Німеччини [Sigen, Duisburg (Prof. Weis), Darmstadt (Prof. Eckert)]. Вказане дозволяє зробити висновок про досить високий рівень забезпечення безпеки інформації у Німеччині. Державною структурою Німеччини, що впроваджує загальнодержавну політику безпеки, є Федеральне Бюро Інформаційної Безпеки (BSI) [2]. Цією структурою було розроблено ряд систем здійснення захищених транзакцій банками. До них відносяться: Захищені електронні транзакції (SET), Електронна готівка (ecash), Кібер Монета (CyberCoin), Мілі-цент (Millicent) та Комп'ютерний Інтерфейс Домашнього Банкінгу (HBCI) [3]. Для реалізації захисту інтернет-банкінгу, тобто для захисту взаємодії між клієнтом та банком, використовують звичайну Інтернет мережу. Часто застосовується протокол Secure Socket Layer (SSL), а також при реалізації цифрового підпису та направленого шифрування криптоперетворення на основі асиметричного криптографічного алгоритму RSA, але уже з ключами довжиною не менше, ніж 2048 біт [4].В якості симетричних крипто перетворень застосовуються симетричні алгоритми шифрування triple-DES та IDEA, а у якості функції гешування RIPEMD-160 [4].

В цілому, Німеччина в частині застосування криптографічних примітивів та протоколів в першу чергу орієнтується на систему стандартизації США та ЄС.

Метою цієї статті є оцінка та порівняльний аналіз якості криптографічного захисту платіжної інформації в банківській сфері Німеччини та України та інтероперабельності в частині захисту інформації на внутрішньому та міжнародному рівнях.

В подальшому під криптографічними системами ми будемо розуміти все, що стосується криптографічних примітивів та протоколів.

1. КРИТЕРІЇ ТА ПОКАЗНИКИ ПОРІВНЯННЯ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

Першим, що є необхідним для оцінки та порівняння криптографічних систем, є вибір критеріїв та показників оцінки криптографічних сис-

тем. Основними стандартами, які розглядаються та аналізуються в цій статті, є стандарти різних рівнів, що застосовуються у Німеччині. В першу чергу це стандарти FIPS 186-3; ISO/IEC 14888-1,2,3; ISO/IEC 18033-1,2,3,4 та FIPS 180-3 [2]. Відносно України, то це стандарти ДСТУ ГОСТ 34.311-2009; ДСТУ ГОСТ 28147-2009, ДСТУ 4145-2002 [5, 6, 7], а також FIPS 186-3 ISO/IEC 14888-1,2,3; ISO/IEC 18033-1,2,3,4 та FIPS 180-3 [8, 9]. Також в якості перспективних розробок будемо розглядати симетричні криптографічні примітиви – блокові симетричні шифри, що розглядались на національному конкурсі в Україні[10].

В подальшому, зважаючи на те, що симетричні та асиметричні криптографічні примітиви та функції гешування мають свої особливості, при їх порівнянні будемо використовувати критерії та показники, які дозволяють врахувати їх специфіку. Так для оцінки криптографічних примітивів запропоновані критерії та показники, за якими здійснюється порівняльний аналіз. Також у відповідності до [11] будемо задавати і основні вимоги блочних симетричних шифрів. Наявність вимог дозволяє застосувати при порівнянні і відповідні критерії.

Для блочних та поточних симетричних шифрів в якості критеріїв та показників порівняння вибрані:

– показник – бітова довжина ключових даних;

– критерій – наявність слабких ключів;

– критерій – стійкість схеми розгортання ключів;

– критерій – стійкість проти атаки груба сила та аналітичних атак.

В якості вимог до блочних симетричних шифрів, висунуті такі:

– повинен розроблятися відкрито та обиратися на міжнародному рівні (бути міжнародним стандартом);

– повинен працювати з блоками та ключами довжиною 128, 256, 512 бітів;

– повинен функціонувати в п'яти основних режимах роботи, що визначені стандартами;

– не мати слабких ключів;

– мати стійку схему розгортання ключів;

– генерування ключів у відповідності до визнаних стандартів.

Для асиметричних крипто перетворень були обрані наступні показники та критерії порівняння:

– показник – бітова довжина ключових даних та вимоги до модуля перетворення;

– критерії – наявності та сутності таємних та відкритих параметрів шифру;

– критерій – стійкість проти «атак на зв'язаних ключах» та атак типу «Повне розкриття»;

– критерій – складність вироблення та перевірки ЕЦП.

В якості вимог до асиметричних перетворень висунуті такі:

– використання модуля перетворення в кільці та полі довжиною не менше, ніж 2048 бітів;

– використання модуля перетворення в групі точок еліптичної кривої довжиною не менше, ніж 192 біта;

– генерування ключів та загальних параметрів у відповідності до визнаних стандартів.

Функції гешування порівнюються за наступними показниками та критеріями:

– показник – розмір блоку повідомлення, що обробляється;

– показник – розмір геш-значення, в яке відображається повідомлення;

– показник – число раундів перетворення;

– показник – максимальна довжина повідомлення, для якої може бути обчислене геш-значення.

В якості загальних вимог до криптографічних примітивів можна висунути наступні:

– алгоритм повинен бути орієнтованим для можливості реалізації на 32-х або 64-х розрядних процесорах;

– зазначені в алгоритмі операції повинні мати по можливості більш ефективну програмну та/або апаратну (апаратно-програмну) реалізацію;

– необхідний для роботи об'єм пам'яті має враховувати можливість реалізації алгоритму у мікро пристроях;

– передбачити можливість паралельного виконання декількох операцій.

Також підкреслимо під критерієм ми будемо розуміти ознаку, на основі якої здійснюється класифікація, оцінка, порівняння, тобто мірило оцінки.

2. РЕЗУЛЬТАТИ ПОРІВНЯННЯ СИМЕТРИЧНИХ КРИПТОСИСТЕМ

Зважаючи на великі обсяги інформації, що обробляються в банківських інформаційних технологіях, як правило, для забезпечення послуг цілісності, справжності та конфіденційності, доцільно застосовувати симетричні криптографічні перетворення.

В табл. 1 та 2 наведені результати порівняння симетричних криптографічних систем: потокових та блокових симетричних шифрів, що застосовуються або можуть застосовуватись в Україні та Німеччині.

З результатів порівняння видно, що в Німеччині діє велика кількість міжнародних стандартів, що надає можливості застосування різних криптографічних систем. В Україні в якості блокового або потокового шифру може використовуватися лише ГОСТ-28147-89 в різних режимах його роботи, при цьому ГОСТ-28147-89 забезпечує тільки задовільний рівень стійкості. Для забезпечення високого та надвисокого рівнів стійкості необхідно застосовувати для внутрішніх систем блоковий симетричний шифр Калина, а на міжнародному AES та SNOW-2. В цьому випадку буде забезпечено не тільки високі рівні стійкості, а і стандартизація та уніфікація і на міжнародному рівні.

Таблиця 1

Порівняння параметрів симетричних криптографічних систем

	Германія			Україна		
Шифр	SNOW-2	TDES	AES	Мухомор	ГОСТ28147-89	Калина
Параметри	Т: Вектор ініціалізації IV, ключ К	Т: Ключі k_1, k_2, k_3	В: Число циклів Т: Ключ К	В: Число циклів Т: Ключ К	В: Число раундів Т: ключ K_c,$K_д$.	В: Число циклів Т: Ключ К
Довжина ключа, біт	К=128, 256 IV=128	168 (3 ключі по 56)	128,192, 256	128-512	K_c= 256 $K_д$ = 512	128, 256, 512

Таблиця 2

Порівняння стійкості симетричних криптографічних систем

	Германія			Україна		
Шифр	SNOW-2	TDES	AES	Мухомор	ГОСТ-28147	Калина
Наявність слабких ключів	Ні	Так	Ні	Ні	Так	Ні
Аналітичні атаки	Ні	2^{113}	Ні	Ні	Так	Ні
Груба сила	2^{256}	2^{168}	$2^{128} – 2^{256}$	2^{512}	2^{64}	2^{512}
Розгортання ключів	Ні	Слабка	Слабка	Ні	Слабка	Ні

3. РЕЗУЛЬТАТИ ПОРІВНЯННЯ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ

Порівняння асиметричних криптосистем зробимо на прикладі «електронних грошей». Сьогодні вони вирішують більшість проблем готівкових грошей. Основними з них є такі як потреба в місці для збереження, складність перевезень, підрахунку, розрахунків за допомогою готівки, конвертація валют, невеликий строк їх служби тощо. Але в той же час при їх використанні постають нові задачі, які потребують вирішення. До них необхідно віднести такі:

– операції банка та клієнта (наприклад домашній банкінг, телефонний банкінг), які використовуються для того, щоб управляти рахунком клієнта;

– угоди клієнт-продавець. Вид операцій, при яких продавець надає клієнту якусь послугу та отримує від нього електронні гроші. До цих операцій відносяться такі, що виконуються за використанням телекомунікаційних систем, наприклад відвідуванням інтернет магазинів;

– угоди клієнт – посередник – продавець. Це тип угод, при яких оплата виконується з використанням якоїсь третьої сторони. Це може бути банк, або кредитна компанія, або інша структура, що є посередником між клієнтом та продавцем.

Аналіз показав, що для Європейських центральних банків особливо важливим є те, щоб громадськість мала довіру до новітніх систем оплати та «електронних грошей». Тому клієнтам має надаватися захист від шахрайства та підробки, в тому числі і шахрайства зі сторони самого банку. Тому в таких системах повинно надаватись також послуги неспростовності об'єктів та суб'єктів взаємодії. Вказане може досягатись на основі використання асиметричних криптографічних перетворень [8]. Крім того, при реалізації криптографічних механізмів та протоколів автентифікації, встановлення, узгодження, передавання та транспортування ключів, розподілу таємниці, тощо, виникає необхідність використання як симетричних, так і асиметричних, так і симетричних крипто перетворень.

В таблиці 3 наведені результати порівняння асиметричних криптографічних систем – міжнародних та регіональних стандартів.

Проаналізуємо в першу чергу відмінності алгоритмів. Так в алгоритмах EC-DSA, EC-GDSA, EC-KCDSA використовується поле GF(p), а в стандарті України ДСТУ 4145-2002 $GF(2^m)$. В алгоритмі EC-KCDSA, на відміну від алгоритмів EC-DSA та EC-GDSA, для перетворення точки еліптичної кривої в ціле число використовується функція гешування.

Таблиця 3

Порівняння параметрів асиметричних криптографічних систем

		EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	RSA	DSA (FIPS-186-3)
Параметри		B:a, b, G, n, f(x), m, U, h, Q				B: D	B: x
		T: d	T: d^{-1}	T: d^{-1}	T: -d	T: E, p, q,ϕ(N)	T: P, q, a
Вимоги до n та d		$n \geq 2^{192}$ $1<d<n-1$			$2^{163} \leq n \leq 2^{509}$ $1<d<n-1$	$n \geq 2^{2048}$ $1<d<n-1$	$2^{511} \leq P \leq 2^{1024}$ $1<x< q-1$
Стійкість проти атак	на зв'язаних ключах	Ні	Неповністю	Так	Ні	Неповністю	
	повне розкриття	$k\sqrt{n}$				$e^{\delta (\ln N)^{\nu} (\ln\ln N)^{1-\nu}}$	

При виробленні електронного цифрового підпису та при його перевірянні в алгоритмах EC-KCDSA та EC-GDSA не виконуються обчислення мультиплікативної інверсії за модулем, що дозволяє зменшити складність вироблення підпису. В свою чергу використання в якості особистого ключа –d в алгоритмі ДСТУ 4145-2002 також дозволяє не обчислювати мультиплікативну інверсію за модулем. В цілому результати аналізу дозволили зробити висновок, що національний стандарт ДСТУ 4145-2002 відповідає міжнародно-визнаним вимогам і може бути застосований для направленого шифрування та встановлення ключів. На відміну від України, Німеччина використовує у якості алгоритми ЕЦП, ще і RSA та DSA, що представлені в FIPS 186 – 3[12].

Результати порівняння складності електронних цифрових підписів наведені в табл. 4.

4. РЕЗУЛЬТАТИ ПОРІВНЯННЯ ФУНКЦІЙ ГЕШУВАННЯ

Для вирішення задач забезпечення цілісності та справжності інформації застосовуються криптографічні контрольні суми[5,13]. Методи формування криптографічних контрольних сум можна розділити на два великі класи: на базі симетричних криптографічних перетворень і на базі асиметричних перетворень,. Такі функції можуть застосовуватися як безпосередньо, так і в інших перетвореннях, це таких, як електронний цифровий підпис, де необхідна ефективна функція відображення повідомлення в образ невеликої фіксованої довжини. Порівняння функцій гешування за запропонованими критеріями наведено в табл. 5.

Необхідно відмітити, що стосовно функцій гешування Німеччина пішла проти світових тенденцій та відмовилась від використання геш – функції SHA-1, що видно з таблиці 5. Замість неї Німеччина стала використовувати функцію гешування RIPEMD-160.

Згідно офіційних публікацій BSI функцію SHA-1 можна використовувати до 2009 року лише для алгоритмів, що пов'язані з підписанням сертифікатів відкритих ключів. До 2010 року SHA-1 може використовуватися лише в алгоритмах підпису сертифікатів відкритих ключів, але тих, що мають не менше 20 бітів ентропії в серійному номері. В подальшому функції гешування RIPEMD-160 та SHA-1 можуть бути застосовані лише для перевірки сертифікатів відкритих ключів. Замість цих функцій, в банках Німеччини будуть застосовуватися сімейство функцій SHA-2 з різними довжинами геш повідомлень.

Також національний інститут стандартизації США (NIST) в результаті появи ряду атак з використанням методу створення колізій на функцію гешування SHA-1, вже в 2007 році розпочав відкритий конкурс на проект нового стандарту гешування, який отримав назву SHA-3.

Що стосується України, то міждержавний стандарт ГОСТ 34.311-95 також припинить свою чинність в 2010 році, тому в Україні доцільно провести роботи з прийняття нового стандарту, а також з впровадження міжнародного стандарту ISO/IEC 10118-3.

5. СТАН ВПРОВАДЖЕННЯ МІЖНАРОДНИХ ТА РЕГІОНАЛЬНИХ СТАНДАРТІВ

Проведений аналіз показав, що Німеччина суттєву увагу приділяє питанням міжнародної та регіональної стандартизації, а також забезпеченню інтероперабельності криптосистем та криптопротоколів. По суті, в реальних системах застосовуються європейські, міжнародні та федеральні стандарти США. Україна також веде деяку роботу в цьому напрямі, але з прийняттям та введенням в дію стандартів велика затримка. В табл. 6 наведені результати порівняльного аналізу стану застосування криптографічних протоколів. Їх результати дозволяють зробити висновок, що Україна суттєво відстає в планів провадження крипто протоколів та їх гармонізації з Європейськими та міжнародними.

Таблиця 4

Складність алгоритмів ЕЦП України і Німеччини

	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ 34.310-2001
Складність вир. ЕЦП	1h+1π+1div+ 2mul+1add+1s	1h+1π+0div+ 2mul+1add+1s	2h+0π+0div+ 1mul+1add+1s	1h+1π+0div+ 2mul+1add+1s	1h+1π+1div+ 2mul+1add+1s
Складність пер. ЕЦП	1h+1π+1div+ 2mul+2s+1sad	1h+1π+1div+ 2mul+2s+1sad	2h+0π+0div+ 0mul+2s+1sad	1h+0π+0div+ 1mul+2s+1sad	1h+1π+1div+ 2mul+2s+1sad

Таблиця 5

Порівняння геш-функцій

Назва геш-функції	SHA-1	SHA 2				RIPEMD-160	ГОСТ 34.311-95
		224	256	384	512		
Рік до якого дійсна	2009	2015	2016	2016	2016	2010	2010
Розмір блоку	512	512	512	1024	1024	512	256
Розмір повідомлення геш	160	224	256	384	512	160	256
Число раундів	80	64	64	80	80	5	1
Максимальна довжина повідомлення	2^{64}-1	2^{64}-1	2^{64}-1	2^{128}-1	2^{128}-1	2^{64}-1	2^{105}

Таблиця 6

Порівняльний аналіз криптографічних систем національних банків України та Німеччини

Критерій	Німеччина	Україна
1) Крипто-примітиви, що використо-вуються в протоколах	– симетричні; – асиметричні; – функції гешування; – функції генерування та перевірки таємних та відкритих парамет-рів	– симетричні; – асиметричні; – функції гешування; – функції генерування та перевірки таємних та відкритих параметрів
2) Види протоколів	– встановлення ключа; – автентифікації; – розподілу спільної таємниці; – вироблення ключа; – обміну; – управління ключовими данними;	– встановлення ключа; – автентифікації; – розподілу спільної таємниці; – вироблення ключа; – обміну;
3) Застосуван-ня протоколів	– програмне забезпечення для аутентифікації, ідентифікації ключів та абонентів; – програмне та апаратне забезпечення конфіденційності, цілісності даних; – розподілення секретів в системах безпеки (протоколи для систе-ми безпеки p2p, Grid Computing); – забезпечення безпеки в групах (в програмах орієнтованих на роботи в групах, та корпоративних мережах); – електронна торгівля (оплати послуг та товарів); – онлайн-банкінг (за допомогою мережі Internet та/або терміналів); – програмне забезпечення для апаратних комплексів, що використовуються для «Довірених обчислень»; – мережева безпека (безпека в середовищах Internet, WAN,WLAN,LAN); – забезпечення безпеки мобільної мережі; – вільне та відкрите ПЗ (OpenPGP); – IP Security Protocol (IPSec) – дистанційне керування доступом та IP-безпека віддаленого досту-пу (ipsra); – виявлення вторгнень; – вироблення ключів в середовищі Internet (kink); – державна інфраструктура відкритих ключів (X.509) та проста інфраструктура відкритих ключів (SPKI); – захист електронної пошти (SMIME); – безпечний протокол мітки часу (STIME); – забезпечення безпеки на транспортному рівні (Transport Layer Security (TLS)); – Веб-безпека транзакцій (wts); – XML цифровий підпис; – національна система; – малі платіжні системи та термінали; – системи електронної готівки та електронних чиків; – електронного документообігу; – електронний уряд.	– програмне забезпечення для ау-тентифікації, ідентифікації ключів та абонентів; – програмне та апаратне забезпечення конфіденційності, цілісності даних; – програмні та апаратні комплекси для розподілення спільних секретів в системах; – мережева безпека (безпека в середо-вищах Internet, WAN,WLAN,LAN); – IP Security Protocol (IPSec); – електронного документообігу; – малі платіжні системи та термінали; – інфраструктура відкритих ключів;
4) Види атак на протоколи:	Атаки на сам протокол: – повтор раніше переданого повідомлення; – маскарад; – віддзеркалення; – на криптографічний примітив; Атаки на його реалізацію: – переповнення буферу пристроя; – помилки при реалізації чи конфігурації обладнання; – ненадійність середи функціонування; – атаки на рівні ядра.	Атаки на сам протокол: – повтор раніше переданого повідом-лення; – маскарад; – віддзеркалення; – на криптографічний примітив; Атаки на його реалізацію: – переповнення буферу пристроя; – помилки при реалізації чи конфігура-ції обладнання; – ненадійність середи функціонування; атаки на рівні ядра.
5) Стандарти протоколів	ISO/IEC 9796-2:2002 ISO/IEC 9796-3:2006 ISO/IEC CD 9797-1 ISO/IEC CD 9797-2 ISO/IEC WD 9797-3 ISO/IEC FDIS 9798-2 ISO/IEC CD 9798-5 ISO/IEC 11770-2:2008 ISO/IEC 11770-3:2008 ISO/IEC 11770-4:2006 ISO/IEC 15946-1:2008 ISO/IEC CD 15946-5 ISO/IEC FCD 19772 ISO/IEC WD 29128 ISO/IEC NP 29146 ISO/IEC TR 14516:2002	ISO/IEC 9796-2:2002 ISO/IEC 9796-3:2006 ISO/IEC CD 9797-1 ISO/IEC CD 9797-2 ISO/IEC WD 9797-3 ISO/IEC FDIS 9798-2 ISO/IEC CD 9798-5 ISO/IEC 11770-2:2008 ISO/IEC 11770-3:2008 ISO/IEC 11770-4:2006 ISO/IEC 15946-1:2008 ISO/IEC CD 15946-5 ISO/IEC FCD 19772 ISO/IEC WD 29128 ISO/IEC NP 29146 ISO/IEC TR 14516:2002

Продовження табл. 6

Критерій	Німеччина	Україна
6) RFC протоколів	Група X9 – Фінансові сервіси. – X9.30: Part 3: Управління сертифікатами – X9.42: Узгодження ключів Діффі-Гелмана – X9.44: Транспортування ключів з використанням RSA – X9.41: Механізм управління сервісами безпеки Група RSA DSI – PKCS #3: Узгодження ключів Діффі-Гелмана – PKCS #7: Синтаксис криптографічних повідомлень Група ECMA: European Computer Manufacturers Association – ECMA-205, Commercially oriented functionality class for security evaluation (COFC), 1st Edition (December 1993)	

ВИСНОВКИ

Результати аналізу та порівняння криптографічних систем України та Німеччини дозволили зробити висновок, що національний банк Німеччини суттєву увагу приділяє впровадженню найбільш перспективних криптографічних примітивів. Німеччина не використовує власної криптографії, а користується міжнародними стандартами. Це дозволяє налагоджувати тісну співпрацю цієї держави з іншими державами світу в різноманітних сферах. Негативним є те, що Німеччина дозволяє використовувати TDES, що не відповідає сучасним вимогам. Але національні стандарти Німеччини BSI вказують шифри, що забезпечують задовільний рівень захищеності. На основі проведеного аналізу були визначені вимоги до можливих строків та умов застосування асиметричних криптографічних перетворень для захисту банківської інформації в Німеччині, а також використання строків та умов в Україні.

Стосовно України можна зробити висновок, що Україна має суттєві досягнення, але відстає в темпах впровадження визнаних міжнародних стандартів, таких як ISO/IEC 9796, ISO/IEC 15946- 2, ISO/IEC 1488 -3, ISO/IEC 18031 та ISO/IEC 18033 тощо. Якщо Україна реально впровадить для захисту банківської інформації симетричні шифри згідно ISO 18033-3,4, а на національному рівні – шифр Калина, то рівень захищеності банківської інформації буде відповідати самим високим міжнародним вимогам.

Одним із способів вирішення питання взаємодії банків різних держав є розділення криптографії на комерційну та державну. Комерційна криптографія повинна засновуватися на однакових стандартах для всього світу, бо сучасний бізнес, а тим паче банківський сектор, часто виходить за рамки окремої держави. Державні ж стандарти криптографічного захисту повинні використовуватися лише для забезпечення потреб держави, а саме для збереження державної таємниці, та оновлюватися з певною періодичністю, в встановлені строки державою.

Література.

[1] http://www.cryptool.org/

[2] http://www.bsi.bund.de/

[3] The IT Security Situation in Germany in 2009, Federal Office for Information Security.

[4] Security Considerations with Electronic Commerce, BSI series on IT security, 2007.

[5] ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Крипто-графическая защита информации. Функция хеширования. Киев. Госстандарт Украины. 1998.

[6] ГОСТ 28147-89 Информационная технология. Криптографическая защита информации. Симметрические алгоритмы шифрования. Киев. Госстандарт Украины. 1989.

[7] ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ, Держстандарт України, 2003.

[8] ISO/IEC 18033-2,3,4 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, Part 3: Block ciphers, Part 4: Stream ciphers, 2005.

[9] ISO/IEC 14888-1,2,3: Information technology – Security techniques – Digital signatures with appendix, 2006.

[10] *Горбенко И.Д.* Отчет по результатам разработки и исследования симметричного блочного алгоритма шифрования «Калина» – спецификация алгоритма «Калина» / И.Д. Горбенко, В.И. Долгов, Р.В. Олейников и др., // Х.: ЗАО «ИИТ», 2007.

[11] *Аулов І.Ф., Кутя Є.Ю., Хряпін Д.Е.* Порівняльний аналіз криптографічних систем національних банків України та Німеччини. //Труды научно-технической конференции КМНТ, часть 1, 2010.

[12] NIST: FIPS Publication 186-3: Digital Signature Standard, June 2009.

[13] ISO/IEC 10118-3 Information technology — Security techniques — Hash-functions

Надійшла до редколегії 18.06.2010.

Горбенко Юрій Іванович, канд. техн. наук, технічний директор ЗАТ «ІІТ». Область наукових інтересів: дослідження механізмів системи електронних цифрових паспортів.

Аулов Іван Федорович, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: дослідження принципів побудування, розгортання та аналізу стійкості криптографічних систем, заснованих на ідентифікаторах.

Кутя Євген Юрійович, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: аналіз асиметричних криптосистем і хеш-функцій, асиметричні криптопримітиви в групі точок еліптичних кривих.

Хряпін Дмитро Едуардович, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: криптоаналітичні властивості БСШ, симетричні криптосистеми та протоколи.

УДК 004.056:[336.71(430)+336.71(477)]

Сравнительный анализ криптографических систем национальных банков Украины и Германии / Ю.И. Горбенко, И.Ф. Аулов, Е.Ю. Кутя, Д.Э. Хряпин // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 404-410.

Приводятся результаты анализа и сравнения криптографических примитивов, применяемых и планируемых к применению для защиты информации в банковских информационных технологиях Украины и Германии.Определен перечень стандартов, предлагается к внедрению и применению на территории Украины.

Ключевые слова: криптографические системы, криптографические примитивы.

Табл. 06. Библиогр.: 05 назв.

UDC 004.056:[336.71(430)+336.71(477)]

Comparative analysis of cryptographic systems of national banks of Ukraine and Germany / Yu.I. Gorbenko, I.F. Aulov, E.Yu. Kutya, D.A. Hryapin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 404-410.

The results of analysis and comparison of cryptographic primitives used and planned to be used for information protection in bank information technologies of Ukraine and Germany are given. A list of standards is determined which is proposed for implementation and use in Ukraine.

Key words: cryptographic systems, cryptographic primitives.

Tab. 06. Ref.: 05 items.

УДК 681.324.067

АНАЛИЗ АВТОКОРРЕЛЯЦИОННЫХ ФУНКЦИЙ СЛУЧАЙНЫХ СИГНАЛОВ

А.А. ТОРБА, В.А. БОБУХ, А.А. ТОРБА

В работе рассматриваются результаты экспериментальных исследований аппаратных генераторов случайных последовательностей и их автокорреляционных функций.

Ключевые слова: автокорреляционная функция, аппаратный генератор случайных последовательностей.

ВВЕДЕНИЕ

Теоретически достижимый уровень скрытности известных криптографических систем в значительной степени определяется статистическими свойствами аппаратного генератора случайных последовательностей (АГСП), построенного на основе физического датчика шума. Этот АГСП используется для формирования ключевых данных, случайных параметров, синхромаркеров и др. Важным свойством АГСП является независимость случайных битовых последовательностей, т.е. формирование каждого следующего случайного бита не зависит от значений всех ранее сгенерированных битов.

Наиболее часто в современных криптографических системах используются датчики шума на основе кремниевых диодов с Зенеровским пробоем [1]. В базовой схеме генерации случайных последовательностей (см. рис. 1) [1] аналоговый случайный сигнал физического датчика шума (с частотой случайных импульсов *Fш*) преобразуется в уровни цифровых сигналов при помощи компаратора с небольшим гистерезисом (TS). Счетный триггер (T) выравнивает вероятности цифрового случайного сигнала. Этот сигнал записывается в сдвигающий регистр RG с частотой *Fo*. Частота – *Fo* – определяет скорость формирования цифровой случайной последовательности. После заполнения сдвигающего регистра параллельный код передается в ПЭВМ.

При тестирование статистических параметров случайной последовательности в ПЭВМ наиболее часто для определения независимости формируемых случайных последовательностей используют автокорреляционный тест [2].

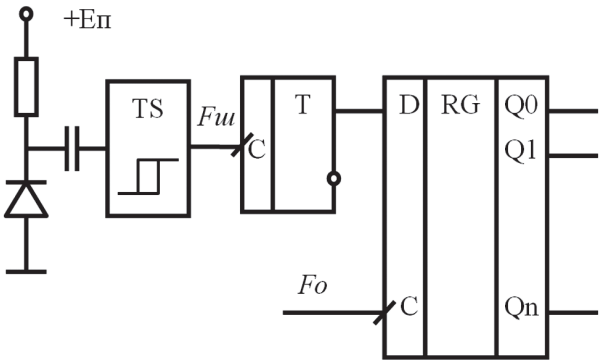


Рис. 1. Базовая схема генерации случайных последовательностей

1. ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СООТНОШЕНИЯ

Для расчета коэффициентов автокорреляционной функции случайной битовой последовательности длиной L_s выбирают начальный участок длиной: $L_a < L_s$. Участок битовой последовательности L_a сдвигают на один бит и сравнивают с исходной битовой последовательностью. Количество битовых сдвигов определяет аргумент – τ – для коэффициентов автокорреляционной функции (на рис. 2 количество сдвигов равно: $\tau = 3$).

Сравнение битовых операндов выполняется логической операцией «ИСКЛЮЧАЮЩЕЕ ИЛИ» (операцией XOR, «суммирование по модулю 2»). При одинаковых битах на входах логического элемента XOR результат сравнения равен логическому нулю, при разных входных битах – результат равен логической единице. Схемы суммирования рассчитывают сумму совпадающих битов – $\Sigma_{\text{совпад}}$ и сумму несовпадающих битов – $\Sigma_{\text{несовп}}$. Коэффициенты автокорреляцион-

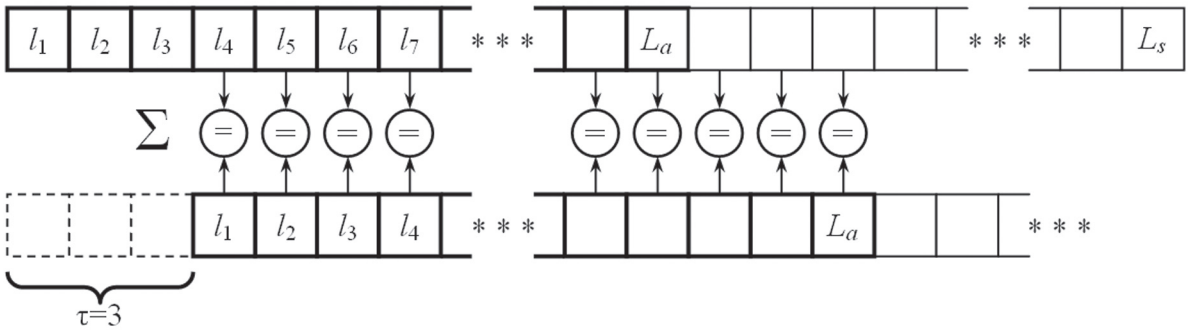


Рис. 2. Алгоритм вычисления автокорреляционной функции

ной функции $K(\tau)$ рассчитываются как разности этих сумм:

$$K(\tau) = \Sigma_{\text{совпад}} - \Sigma_{\text{несовп}}, \quad (1)$$

где: τ – количество битовых сдвигов случайной последовательности.

Обычно подсчитывают только количество единичных битов на выходе элементов XOR (т.е. количество несовпадений), поэтому:

$$K(\tau) = L_a - 2 \cdot \Sigma_{\text{несовп}}. \quad (2)$$

Коэффициент автокорреляционной функции при нулевой задержке ($\tau = 0$) численно равен дисперсии случайного процесса, поэтому (с учетом полного совпадения всех битов) дисперсия равна:

$$K(0) = D = L_a. \quad (3)$$

Нормированные коэффициенты автокорреляционной функции :

$$k(\tau) = K(\tau) / K(0) - \quad (4)$$

всегда меньше единицы.

Нормированные коэффициенты автокорреляционной функции можно рассчитать по условным вероятностям переходов случайных битов в последовательности (рис. 3). Вероятности формирования случайных битов: $P(x0) = P(x1) = 0{,}5$. Вероятности формирования следующего случайного бита: $P(x^+0) = P(x^+1) = 0{,}5$.

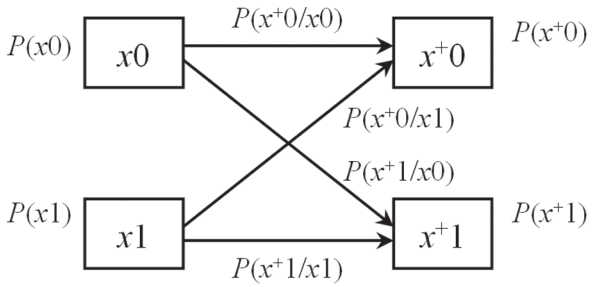


Рис. 3. Вероятности переходов случайных битов

Условные вероятности перехода следующего бита в противоположное состояние: $P(x^+0/x1) = P(x^+1/x0)$.

Условные вероятности сохранения предыдущего состояния бита: $P(x^+0/x0) = P(x^+1/x1)$.

В этих соотношениях учитывается:

$$P(x^+0/x0) + P(x^+1/x0) = 1, \quad (5)$$

потому что после нулевого предыдущего бита ($x0$) будет переход или в нулевое состояние (x^+0), или в единичное состояние (x^+1) с суммарной вероятностью, равной единице.

Аналогично:

$$P(x^+1/x1) + P(x^+0/x1) = 1. \quad (6)$$

При формировании независимых соседних случайных битов условные вероятности равны:

$$P(x^+0/x1) = P(x^+1/x0) = P(x^+0/x0) = P(x^+1/x1) = 0{,}5. \quad (7)$$

При наличии корреляционных связей между соседними случайными битами условные вероятности различны:

$$P(x^+1/x1) - P(x^+0/x1) = P(x^+0/x0) - P(x^+1/x0) = \varepsilon. \quad (8)$$

Величина разности условных вероятностей – ε – меньше единицы по модулю и может принимать положительные или отрицательные значения. Для статистически независимых случайных битов эта разность равна нулю: $\varepsilon = 0$.

С учетом соотношений (1), (3), (4), (5), (6), (8) нормированные коэффициенты автокорреляционной функции равны:

$$k(\tau) = [P(x0) \cdot P(x^+0/x0) + P(x1) \cdot P(x^+1/x1)] - [P(x0) \cdot P(x^+1/x0) + P(x1) \cdot P(x^+0/x1)] = \varepsilon(\tau), \quad (9)$$

где: $P(x0) \cdot P(x^+0/x0) = P(x0, x^+0)$ – вероятность сохранения нуля; $P(x1) \cdot P(x^+1/x1) = P(x1, x^+1)$ – вероятность сохранения единицы; $P(x0) \cdot P(x^+1/x0) = P(x0, x^+1)$ – вероятность перехода из нуля в единицу; $P(x1) \cdot P(x^+0/x1) = P(x1, x^+0)$ – вероятность перехода из единицы в нуль.

2. ОПРЕДЕЛЕНИЕ СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ СЛУЧАЙНЫХ БИТОВ

Условием статистической независимости генерируемых случайных битов является равенство всех условных вероятностей (7) или нулевое значение разности этих вероятностей: $\varepsilon(\tau) = 0$.

В экспериментальных измерениях понятие вероятности справедливо только для бесконечно большой последовательности случайных битов. Для ограниченной последовательности статистическим критерием независимости является попадание коэффициентов автокорреляционной функции в доверительный интервал $\pm 3\sigma$ с доверительной вероятностью $\alpha = 0{,}99$ [2].

В наших экспериментах длина последовательности выбиралась: $L_a = 1\,000\,000$ бит. С учетом соотношения (2) дисперсия автокорреляционной функции также равна: $D = L_a = 1\,000\,000$. Среднеквадратичное отклонение: $\sigma = \sqrt{D} = 1000$.

Поэтому при попадании коэффициентов автокорреляционной функции $K(\tau)$ в доверительный интервал ± 1000 можно утверждать о статистической независимости случайных битов с задержками, равной τ или более.

На рис. 4 приведены коэффициенты автокорреляционной функции, нормированные на величину среднеквадратичного отклонения $\sigma = 1000$. Скорость формирования случайных битов $Fo = 11$ МГц значительно превышает частоту шумовых импульсов диода с Зенеровским пробоем: $Fш = 3{,}8$ МГц.

Обратите внимание – форма графика напоминает известную функцию: $y = \sin(x) / x$. При величине задержки $\tau \geq 21$ все коэффициенты попадают в доверительный интервал ± 3, т.е. случайные биты, разнесенные на временной интервал: $t \geq 21 / Fo$, – не имеют корреляционных связей.

Аналогичные результаты получаются при исследовании влияния скорости формирования случайных последовательностей *Fo* на их статистические свойства.

На рис. 5 показаны экспериментальные зависимости коэффициентов автокорреляционной функции K(1), K(2) и K(3) (нормированных на величину среднеквадратичного отклонения $\sigma = 1000$) от безразмерного параметра: $m = Fш / Fo$.

Для коэффициента K(1) экспериментальная зависимость практически повторяет график на рис. 4 и условие статистической независимости соседних случайных битов (т.е попадание коэффициентов автокорреляционной функции в доверительный интервал $\pm 3\sigma$) наступает при скорости формирования *Fo* меньшей в 7,5 раз, чем частота шумовых импульсов *Fш* на выходе датчика (при $m_{кр} = Fш / Fo = 7{,}5$).

При величине $m = Fш / Fo = 1$ значение коэффициента автокорреляционной функции K(1) имеет отрицательное значение (см. рис. 5), потому что на вход счетного триггера T (см. рис. 1) за время формирования следующего бита поступает в среднем один случайный импульс от датчика шума и состояние счетного триггера изменяется на противоположное. Поэтому количество несовпадений соседних битов будет значительно больше, чем количество совпадений.

При величине $m = Fш / Fo = 2$ значение коэффициента K(1) имеет положительное значение, потому что на вход счетного триггера T за время формирования следующего бита поступает в среднем два случайных шумовых импульса и состояние счетного триггера после двух инверсий совпадает с предыдущим значением. Количество совпадений соседних битов будет значительно больше, чем несовпадений.

Аналогичные изменения знака коэффициента автокорреляционной функции K(1) происходят и для последующих четных и нечетных значений безразмерного параметра *m*.

График зависимости K(2) от *m* повторяет график для коэффициента K(1), но сжат влево по горизонтали в два раза. Поэтому условие статистической независимости наступает при большей в два раза скорости формирования случайных битов *Fo* или меньшем в два раза параметре *m* (на рис. 5 эти условия отмечены эллипсами в таблице).

Аналогично: график зависимости K(3) от *m* сжат по горизонтали в три раза и условие независимости наступает при трехкратной скорости формирования.

На основе анализа этих графиков можно утверждать: если скорость формирования случайных битов соответствует условию независимости для единичной задержки: $|K(1)| < 3\sigma$, то коэффициенты автокорреляционной функции с большими задержками также будут удовлетворять условию независимости.

3. ОБЪЕДИНЕНИЕ ПОТОКОВ НЕЗАВИСИМЫХ СЛУЧАЙНЫХ СИГНАЛОВ

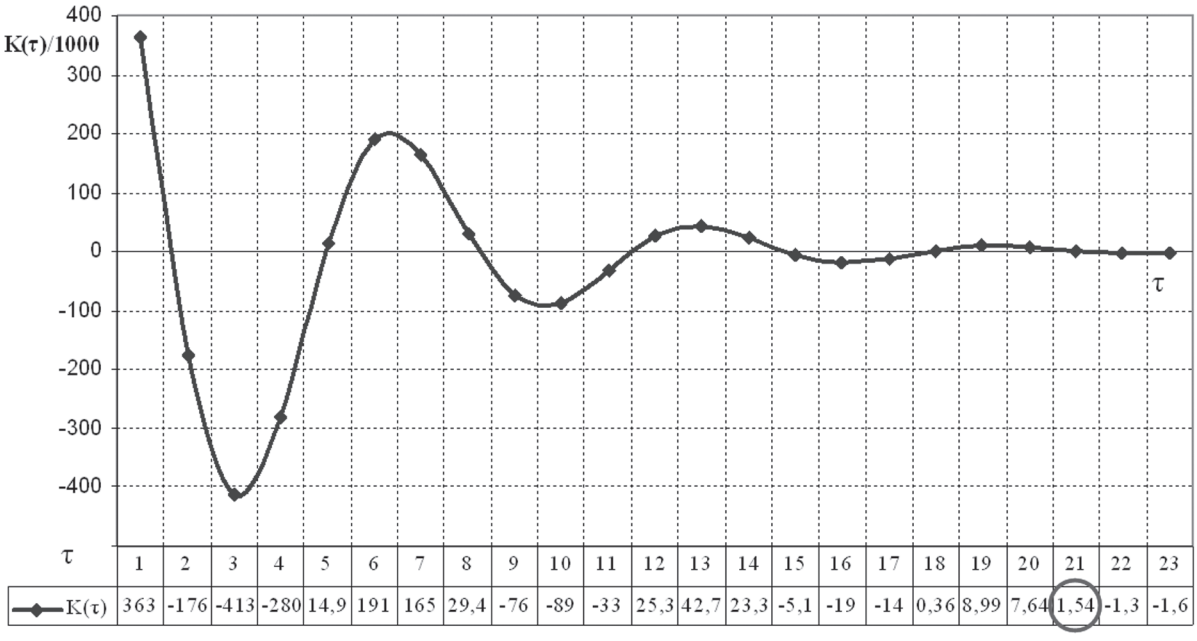
В патенте Украины № 61439 [3] предложено объединять логическим элементом XOR потоки независимых случайных сигналов (рис. 6), раздвинутых во времени многоразрядным сдвигающим регистром RG1.

Если у регистра RG1 только два отвода, то коэффициенты автокорреляционной функции для выходного случайного сигнала можно рассчитать по формуле (2):

$$K(\tau) = L_a - 2\sum (l_i \oplus l_{i+m}) \oplus (l_{i+\tau} \oplus l_{i+m+\tau}), \qquad (10)$$

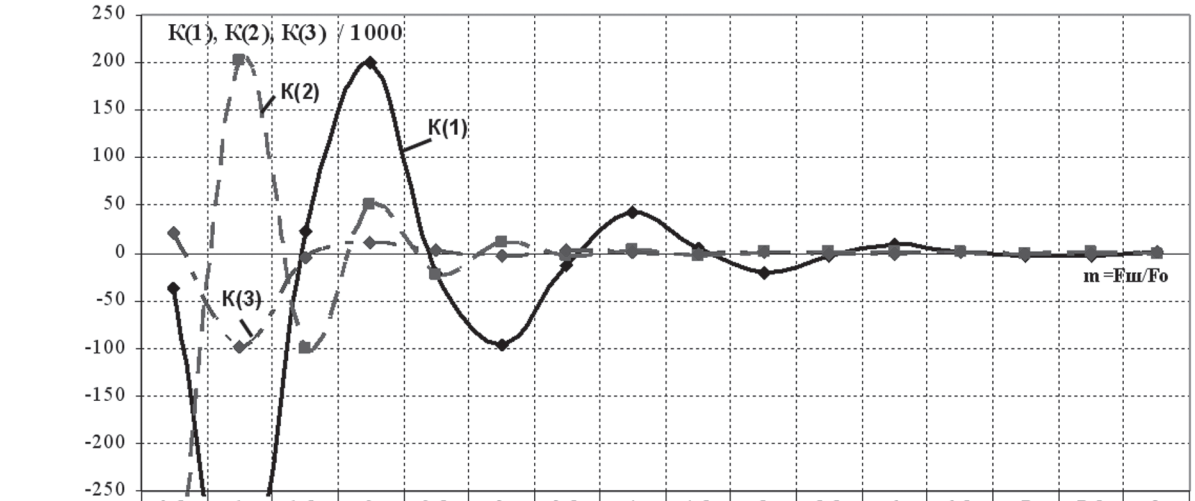
где: *m* – количество разрядов между отводами регистра.

В этой формуле учтено, что два случайных сигнала (сдвинутых во времени на количество



τ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
K(τ)	363	-176	-413	-280	14,9	191	165	29,4	-76	-89	-33	25,3	42,7	23,3	-5,1	-19	-14	0,36	8,99	7,64	1,54	-1,3	-1,6

Рис. 4. Коэффициенты автокорреляционной функции



m =Fш/Fo	0,5	1	1,5	2	2,5	3	3,5	4	4,5	5	5,5	6	6,5	7	7,5	8
K(1)	-37	-404	22,8	201	-21,2	-96	-12,1	43,2	5,8	-20,7	-3,9	8,1	0,8	-3,2	-2,1	0,8
K(2)	-389	203	-100	50,5	-23,7	10,4	-2,2	3	-2,2	1,5	0,1	0,4	0,8	-0,8	0,1	-0,4
K(3)	21	-97,8	-4,7	11,6	2,9	-2,7	2,4	1,5	-0,6	0,01	-1,1	-0,8	0,1	-0,7	-0,7	0,1

Рис. 5. Зависимости коэффициентов $K(1)$, $K(2)$ и $K(3)$ от безразмерного параметра: $m = Fш / Fo$.

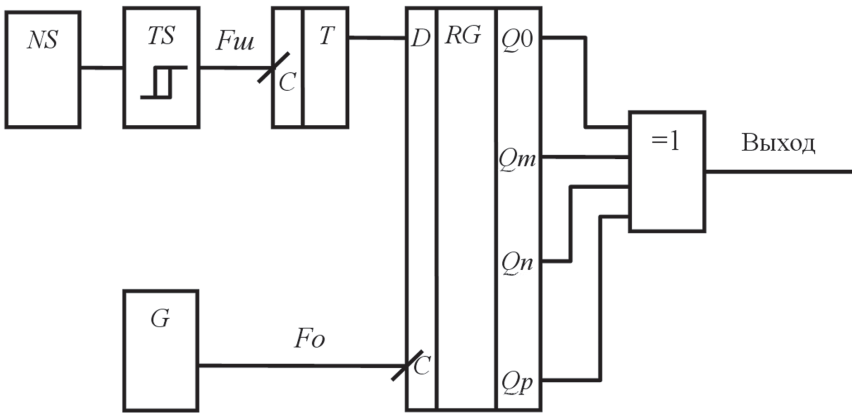


Рис. 6. Объединение независимых потоков случайных сигналов на отводах регистра элементом XOR

разрядов m) объединяются логическим элементом XOR и при вычислении коэффициентов автокорреляционной функции также используется сдвиг на количество разрядов τ с последующим объединением логической функцией XOR.

Используя сочетательный закон алгебры логики, уравнение (10) можно переписать в виде:

$$K(\tau) = L_a - 2\sum(l_i \oplus l_{i+\tau}) \oplus (l_{i+m} \oplus l_{i+m+\tau}). \quad (11)$$

В соответствии с этой формулой можно сначала рассчитать коэффициенты автокорреляционной функции отдельно для сигнала с первого отвода регистра (см. верхний ряд элементов сравнения на рис. 7), затем рассчитать коэффициенты автокорреляционной функции для сигнала со второго отвода (см. нижний ряд элементов сравнения на рис. 7), а потом «сложить по модулю 2» эти коэффициенты (см. средний ряд элементов сравнения на рис. 7).

Вероятности логических сигналов на выходах верхнего ряда (или нижнего ряда) элементов сравнения на рис. 7 равны:

$$P(0) = [P(x0) \cdot P(x^+0/x0) + P(x1) \cdot P(x^+1/x1)];$$

$$P(1) = [P(x0) \cdot P(x^+1/x0) + P(x1) \cdot P(x^+0/x1)].$$

Разность этих вероятностей в соответствии с уравнением (9) равна:

$$P(0) - P(1) = \varepsilon.$$

Поэтому можно записать: $P(0) = P(1) + \varepsilon$.

В табл. 1 приведены комбинации логических сигналов на входах логических элементов XOR для среднего ряда (см. рис. 7) и вероятности этих сигналов с учетом их статистической независимости.

Таблица 1

Входные сигналы		Вероятности
0	0	$[P(1) + \varepsilon] \cdot [P(1) + \varepsilon]$
0	1	$[P(1) + \varepsilon] \cdot P(1)$
1	0	$P(1) \cdot [P(1) + \varepsilon]$
1	1	$P(1) \cdot P(1)$

На выходах логических элементов XOR в среднем ряду (см. рис. 7) будет формироваться ло-

гический нуль при равенстве входных логических сигналов. Это соответствует первой и последней строкам в табл. 1.

Поэтому вероятность логического нуля на выходах элементов XOR равна:

$$P''(0) = [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] + P(1) \cdot P(1).$$

Выходная логическая единица на выходах элементов XOR в среднем ряду соответствует второй и третьей строке в табл. 1.

Вероятность логической единицы на выходах элементов XOR равна:

$$P''(1) = [P(1) + \varepsilon] \cdot P(1) + P(1) \cdot [P(1) + \varepsilon].$$

Разность вероятностей на выходе элементов XOR в среднем ряду численно равна нормированным коэффициентам автокорреляционной функции для схемы с объединением независимых потоков случайных сигналов на двух отводах сдвигающего регистра:

$$k'' = \varepsilon'' = P''(0) - P''(1) = [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] +$$
$$+P(1) \cdot P(1) - [P(1) + \varepsilon] \cdot P(1) - P(1) \cdot [P(1) + \varepsilon] = \varepsilon^2. \quad (12)$$

Из этого равенства следует: если нормированные коэффициенты автокорреляционной функции для исходного сигнала без объединения независимых потоков: $k(\tau) = \varepsilon(\tau)$ – меньше единицы, то квадрат этой величины будет еще значительно меньше.

В общем случае – при разных значениях коэффициентов автокорреляционной функции у объединяемых независимых потоков случайных сигналов – необходимо умножать эти коэффициенты отдельно для каждой задержки τ:

$$k''(\tau) = k_1(\tau) \cdot k_2(\tau). \quad (13)$$

В табл. 2 приведены комбинации логических сигналов для схемы с объединением трех отводов сдвигающего регистра трехвходовым элементом XOR (см. рис. 6) и вероятности этих сигналов с учетом их статистической независимости.

Таблица 2

Входные сигналы			Вероятности
0	0	0	$[P(1) + \varepsilon] \cdot [P(1) + \varepsilon] \cdot [P(1) + \varepsilon]$
0	0	1	$[P(1) + \varepsilon] \cdot [P(1) + \varepsilon] \cdot P(1)$
0	1	0	$[P(1) + \varepsilon] \cdot P(1) \cdot [P(1) + \varepsilon]$
0	1	1	$[P(1) + \varepsilon] \cdot P(1) \cdot P(1)$
1	0	0	$P(1) \cdot [P(1) + \varepsilon] \cdot [P(1) + \varepsilon]$
1	0	1	$P(1) \cdot [P(1) + \varepsilon] \cdot P(1)$
1	1	0	$P(1) \cdot P(1) \cdot [P(1) + \varepsilon]$
1	1	1	$P(1) \cdot P(1) \cdot P(1)$

Логический сигнал на выходе элемента XOR будет равен нулю при четном количестве входных единичных битов. Это соответствует первой, четвертой, шестой и седьмой строкам табл. 2. Вероятность логического нуля на выходе элемента XOR равна сумме вероятностей в этих строках.

Логическая единица на выходе элемента XOR соответствует второй, третьей, пятой и восьмой строкам табл. 2.

Нормированные коэффициенты автокорреляционной функции для каждой задержки τ численно равны разности этих вероятностей:

$$k'' = \varepsilon'' = [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] +$$
$$+[P(1) + \varepsilon] \cdot P(1) \cdot P(1) + P(1) \cdot [P(1) + \varepsilon] \cdot P(1) +$$
$$+ P(1) \cdot P(1) \cdot [P(1) + \varepsilon] - [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] \cdot$$
$$P(1) - [P(1) + \varepsilon] \cdot P(1) \cdot [P(1) + \varepsilon] - P(1) \cdot$$
$$\cdot [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] - P(1) \cdot P(1) \cdot P(1) = \varepsilon^3. \quad (14)$$

Аналогично можно показать, что для схемы с объединением четырех отводов сдвигающего регистра четырехвходовым элементом XOR нормированные коэффициенты автокорреляционной функции численно равны :

$$k'' = \varepsilon'' = \varepsilon^4. \quad (15)$$

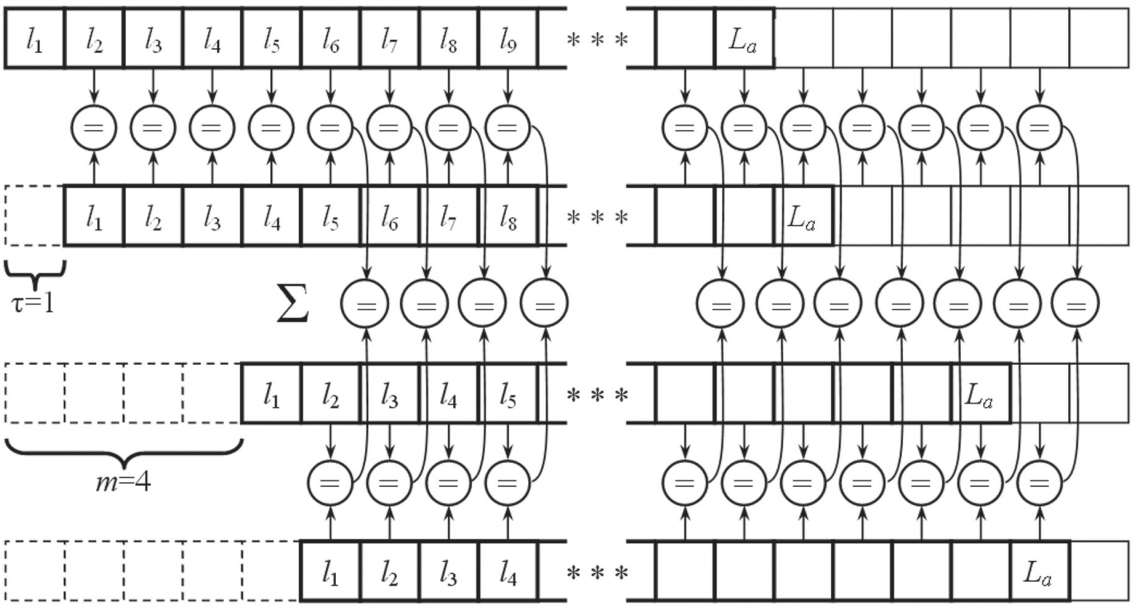


Рис. 7. Алгоритм вычисления автокорреляционной функции для регистра с объединением двух отводов элементом XOR

На рис. 8 приведены результаты измерений зависимости коэффициента автокорреляционной функции $K(1)$ от безразмерного параметра $m = Fш / Fo$ для исходного потока без объединений (график $n = 1$) и зависимости коэффициента $K(1)$ для объединения двух потоков элементом XOR ($n=2$), трех потоков ($n=3$) и четырех потоков ($n=4$) на отводах сдвигающего регистра (см. рис. 6).

Обратите внимание – коэффициенты $K(1)$ для регистра с двумя отводами ($n = 2$) имеют только положительные значения (в соответствии с уравнением (12)), и форма графика соответствует квадрату графика исходной зависимости ($n = 1$).

Нормированные значения коэффициентов автокорреляционной функции $k(1) = K(1) / D$ всегда меньше единицы. В наших экспериментах $D = L_a = 1\,000\,000$. Поэтому абсолютные значения в таблице в нижней части рис. 8 необходимо поделить на 1000.

Аналогично – форма графика для регистра с тремя отводами ($n = 3$) соответствует кубу исходной зависимости, а для графика ($n = 4$) форма соответствует четвертой степени графика исходной зависимости.

Полученные нормированные значения коэффициентов автокорреляционной функции соответствуют уравнениям (12), (14), (15).

Важный практический результат, полученный на основе анализа зависимостей коэффициентов автокорреляционной функции на рис. 8, – это возможность увеличения скорости формирования случайных битов (Fo) в два раза для регистра с двумя отводами (на рис. 8 условия независимости в таблице обведены окружностями).

Для схемы с тремя отводами и объединением случайных независимых потоков трехвходовым элементом XOR скорость формирования Fo можно увеличить в три раза при сохранении условия независимости всех формируемых случайных битов.

В общем случае можно утверждать: для схемы (рис. 6) с количеством отводов n можно увеличить скорость формирования в n раз.

При объединении элементом XOR статистически независимых потоков с различными автокорреляционными функциями их результирующие нормированные коэффициенты равны произведению исходных коэффициентов для каждой задержки τ. На рис. 9 показаны коэффициенты автокорреляционных функций для двух независимых сигналов: исходной схемы формирования случайных битовых последовательностей ($k_1(\tau)$) и схемы с детерминированными перестановками битов ($k_2(\tau)$) [4].

В соответствии с уравнением (13) для каждой задержки τ коэффициенты результирующей автокорреляционной функции $k''(\tau)$ меньше, чем наименьший из коэффициентов исходных автокорреляционных функций $k_1(\tau)$ или $k_2(\tau)$, потому что наименьший из коэффициентов умножается на число, меньшее единицы. Это утверждение справедливо для значений модуля коэффициентов автокорреляционных функций (без учета знака).

ВЫВОДЫ

На основе анализа результатов исследований автокорреляционных функций выходных сигналов АГСП с датчиками шума на основе кремниевых диодов с Зенеровским пробоем можно сделать следующие выводы:

• Условием статистической независимости генерируемых случайных битов является равенство всех условных вероятностей переходов соседних случайных битов или нулевое значение разности этих вероятностей: $\varepsilon(\tau) = 0$;

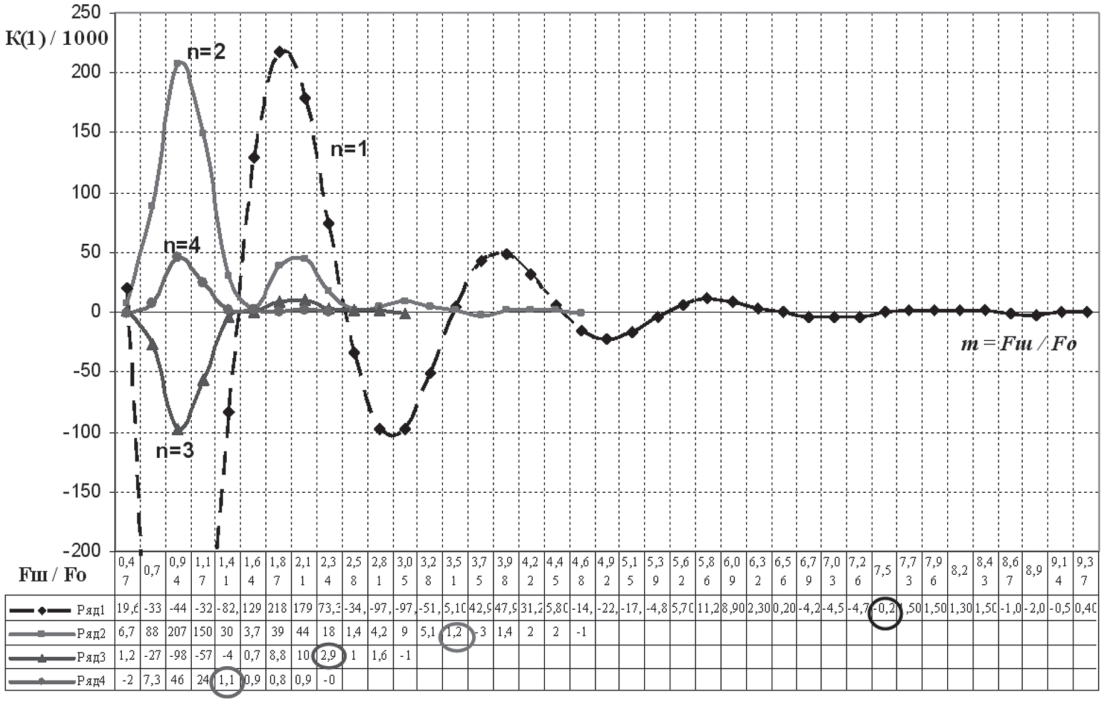


Рис. 8. Зависимости коэффициентов автокорреляционной функции $K(1)$ для регистра с отводами

Рис. 9. Нормированные автокорреляционные функции для сигналов с объединением элементом XOR

• Для ограниченной последовательности случайных битов статистическим критерием независимости является попадание коэффициентов автокорреляционной функции в доверительный интервал $\pm 3\sigma$ с доверительной вероятностью $\alpha = 0{,}99$;

• Объединение потоков независимых случайных последовательностей элементом XOR (сумматором по модулю 2) уменьшает модули нормированных коэффициентов автокорреляционных функций и, в конечном итоге, позволяет повысить скорость формирования случайных последовательностей.

Литература.

[1] *А.А. Торба, С.Г. Елаков, А.З. Степченко.* Генерация равновероятных случайных последовательностей на основе физических датчиков // Радиотехника. Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119, с.108-113.

[2] *А. Менезис, П. ван Оршоа, С. Ватсон,* Руководство по прикладной криптографии – CRC: Press, 1996. – 816 с.

[3] Декларационный патент Украины № 61439 А, Бюл. № 11 от 17.11.2003.

[4] Патент Украины № 86979, Бюл. № 11 от 10.06.2009.

Поступила в редколлегию 22.06.2010.

Торба Александр Алексеевич, кандидат технических наук, доцент кафедры ЭВМ ХНУРЭ. Область научных интересов: аппаратные средства криптографических систем.

Бобух Всеволод Анатольевич, кандидат технических наук, начальник отдела аппаратных средств защиты информации ЗАО «ИИТ», старший научный сотрудник кафедры БИТ ХНУРЭ. Область научных интересов: апаратные средства систем защиты информации.

Торба Анна Александровна, ассистент кафедры ПО ЭВМ, ХНУРЭ. Область научных интересов: аппаратно-программные средства криптографических систем.

УДК 681.324.067

Аналіз автокореляційних функцій випадкових сигналів / А.А. Торба, В.А. Бобух, Г.О. Торба // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 411-417.

У статті було розглянуто результати експериментальних досліджень апаратних генераторів випадкових послідовностей та їх автокореляційних функцій.

Ключові слова: автокореляційна функція, апаратний генератор випадкових послідовностей.

Табл. 02. Іл.09. Бібліогр.: 04 найм.

UDC 681.324.067

Analysis of autocorrelation functions of random signals / A.A. Torba, V.A. Bobukh, A.A. Torba // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 411-417.

Results of experimental researches of hardware generators of random sequences and their autocorrelation functions are considered in the paper.

Key words: autocorrelation function, hardware random sequences generator.

Tab. 02. Fig. 09. Ref.: 04 items.

УДК 003.26

ИЗОМОРФИЗМ ДИВИЗОРОВ И ПАР ТОЧЕК ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ РОДА ДВА

А.В. БЕССАЛОВ, А.В. НЕЛАСАЯ

Обсуждается вопрос представления дивизора гиперэллиптической кривой точками в расширении основного поля. Раскрывается связь между точками, образующими дивизор, для гиперэллиптической кривой второго рода.

Ключевые слова: гиперэллиптическая кривая, род кривой, дивизор, форма Мамфорда, изоморфизм.

ВВЕДЕНИЕ

Развитие методов асимметричной криптографии обусловило переход от криптографических преобразований в кольцах и конечных полях к использованию арифметики в группе точек эллиптической кривой. Эллиптическая криптография, кроме традиционных криптосистем, основанных на проблеме дискретного логарифмирования на эллиптической кривой, стала основой для построения криптосистем с новыми свойствами. В частности, в последние два десятилетия были предложены криптосистемы, основанные на спариваниях точек эллиптических кривых и криптосистемы на гиперэллиптических кривых. Гиперэллиптические кривые – это кривые более высокого рода, которые являются обобщением понятия эллиптической кривой. При этом, если билинейная криптография ведет в сторону супербольших полей (до десятков килобит), то гиперэллиптические кривые дают реальную перспективу использовать малые поля (десятки бит). Ясно, что такая перспектива является привлекательной, и поэтому активно исследуется учеными мира.

Точки гиперэллиптической кривой, в отличие от точек эллиптической кривой, не образуют группу. Формальные суммы точек называются дивизорами. Количество входящих в дивизор точек называют весом дивизора. В качестве групповой структуры рассматривается якобиан кривой, который представляет собой факторгруппу дивизоров нулевой степени по подгруппе главных дивизоров (дивизоров функций) [1]. Представителем каждого класса рассматриваемой факторгруппы является приведенный дивизор, который может быть записан в виде двух полиномов в форме Мамфорда [2]. Аналогично операции сложения точек эллиптической кривой введена операция сложения дивизоров гиперэллиптической кривой, которая, однако, является гораздо более сложной [3].

Естественно было ожидать, что более сложный математический аппарат может повысить безопасность криптосистемы. Однако при всей сложности аппарата очень скоро стало известно, что гиперэллиптические кривые подвержены атаке исчисления индексов. При этом проблема дискретного логарифмирования из экспоненциальной упрощается до субэкспоненциальной. Причем эффективность такой атаки растет с возрастанием рода кривой. В этой связи сегодня наиболее перспективными для криптографических приложений считаются кривые рода 2 и 3.

Для разработчиков криптосистем одним из приоритетов всегда является вопрос эффективности. Основная задача при этом – сократить объем используемой памяти и увеличить скорость криптографических преобразований. С целью увеличения скорости преобразований исследования ведутся в направлении оптимизации групповой операции. Разными разработчиками представлены явные формулы сложения и удвоения дивизоров (например [4, 5]).

Что касается памяти, сразу же возникает вопрос: каким образом записывать элемент (дивизор) гиперэллиптической кривой? Оказывается, он имеет размер, например, для кривой второго рода, в два раза превосходящий размер элемента для эллиптической кривой. Если точка эллиптической кривой имеет две координаты (x,y), то для хранения дивизора уже нужно хранить четыре параметра. Каждый из них имеет размер в два раза меньше координаты точки эллиптической кривой, но в общей сложности он остается таким же.

Целью данной статьи является исследование возможности оптимизации представления дивизора гиперэллиптической кривой второго рода с помощью координат входящих в него точек.

1. ПРЕДСТАВЛЕНИЕ ДИВИЗОРА ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Каждый элемент якобиана гиперэллиптической кривой, определенной над $GF(p)$, представляется двумя полиномами в форме Мамфорда с коэффициентами из $GF(p)$. Однако координаты точек, входящих в дивизор, в этом случае определены в $GF(p^g)$. Рассмотрим связь между точками, входящими в дивизор, и его представлением парой полиномов.

Пусть имеем гиперэллиптическую кривую

$$C: y^2 + h(x)y = f(x),$$

для которой полиномы $h(x)$, $f(x)$ со степенями $\deg h(x) < g$, $\deg f(x) = 2g + 1$ определены над полем $\boldsymbol{F}_p$, $p > 3$. Рассмотрим кривую рода $g = 2$ со старшей степенью $\deg f(x) = 5$. Координаты точки (X,Y) кривой C, определяющие якобиан гиперэллиптической кривой (ГЭК) рода 2, лежат в поле $\boldsymbol{F}_p$ и в расширении $\boldsymbol{F}_p^2$. Справедливо

Утверждение 1. Для любой точки $P = (X, Y)$ в расширении $\boldsymbol{F}_p^2$ существует сопряженная точка $\tilde{P} = (\tilde{X}, \tilde{Y})$, такая, что приведенный дивизор их суммы в форме Мамфорда

$$D[P + \tilde{P}] = <a(x), b(x)> \qquad (1)$$

однозначно представляется параболой и уравнением прямой

$$a(x) = (x - X)(x - \tilde{X}) = x^2 + Ax + B, \qquad (2)$$

$$b(x) = Y\frac{x - \tilde{X}}{X - \tilde{X}} + \tilde{Y}\frac{x - X}{\tilde{X} - X} = Gx + H, \qquad (3)$$

где коэффициенты A, B, G, $H \in \boldsymbol{F}_p$. Полином $a(x)$ несет информацию об x-координатах точек P и $\tilde{P}$, а $b(x)$ – об их y-координатах.

Доказательство. Пусть известны координаты точки $P = (X, Y)$ в расширении $\boldsymbol{F}_p^2$ с неприводимым полиномом $\psi(x) = t^2 + a_1 t + a_0$

$$X = ct + d, \quad Y = et + f. \quad c, e \neq 0. \qquad (4)$$

Определим координаты сопряженной точки

$$\tilde{X} = \tilde{c}t + \tilde{d}, \quad \tilde{Y} = \tilde{e}t + \tilde{f}. \qquad (5)$$

Из (2) следует

$$X + \tilde{X} = (c + \tilde{c})t + d + \tilde{d},$$

$$X\tilde{X} = (c\tilde{c}t^2 + (c\tilde{d} + \tilde{c}d)t + d\tilde{d}) \bmod \psi(t).$$

Так как правые части этих равенств лежат в поле $\boldsymbol{F}_p$, то отсюда следует

$$\tilde{A} = -A \bmod p,$$

$$\frac{\tilde{d} - d}{c} = -a_1 \bmod p \Rightarrow \tilde{d} = (d - a_1 c) \bmod p.$$

Подставляя эти параметры в (5), легко выразить координаты сопряженной точки как

$$\tilde{X} = X(\tau) = c\tau + d, \quad \tilde{Y} = Y(\tau) = e\tau + f, \qquad (6)$$

с линейной заменой переменной

$$\tau = (-t - a1) \bmod p. \qquad (7)$$

Таким образом, точки P и $\tilde{P}$ связаны простой заменой переменной. Ясно, что для каждой точки P в расширении $\boldsymbol{F}_p^2$ существует единственная сопряженная точка $\tilde{P}$, и эта пара точек единственным образом определяет полиномы (2) и (3) приведенного дивизора (1). Доказательство завершено.

Обратная задача – нахождение координат точек P и $\tilde{P}$ при заданном в полиномиальной форме дивизоре – требует на первом этапе решения квадратного уравнения в правой части (2) в расширении $\boldsymbol{F}_p^2$. Дискриминант этого уравнения

$$\Delta = (A2 - 4B) \bmod p \qquad (8)$$

является квадратичным вычетом или невычетом в поле $\boldsymbol{F}_p$. В первом случае получаем x-координаты двух точек кривой $\boldsymbol{C}$ над $\boldsymbol{F}_p$

$$X_{1,2} = \frac{-A \pm \sqrt{\Delta}}{2}, \qquad (9)$$

во втором случае – координаты сопряженных точек кривой $\boldsymbol{C}$ над расширением $\boldsymbol{F}_p^2$. Выразим в последнем случае

$$\Delta = (\alpha t + \beta)2 \bmod (t2 + a1t + a0) =$$
$$= \alpha 2(a12/4 - a0) \bmod p.$$

Отсюда определяем

$$\beta = \frac{a_1 \alpha}{2} \bmod p, \quad \alpha^2 = \frac{4\Delta}{a_1{}^2 - 4a_0} \bmod p. \qquad (10)$$

Тогда с учетом равенства $\sqrt{\Delta} = \alpha(t + \frac{a_1}{2})$ получим x-координаты сопряженных точек P и $\tilde{P}$

$$X = \frac{-A + \alpha(t + \frac{a_1}{2})}{2}, \quad \tilde{X} = \frac{-A - \alpha(t + \frac{a_1}{2})}{2}. \qquad (11)$$

Их y-координаты легко находятся из равенств

$$Y = b(X), \qquad \tilde{Y} = b(\tilde{X}). \qquad (12)$$

Пример 1. Рассмотрим кривую 2-го рода $y^2 = (x^5 + 2x^2 + x + 3) \bmod 7$ с неприводимым полиномом $\psi(x) = t^2 - t - 1$ ($a_1 = -1$) в расширении $\boldsymbol{F}_p^2$. Для известной точки $P = (5t + 6, 2t + 4)$ найдем сопряженную точку $\tilde{P}$ и приведенный дивизор их суммы. Согласно (6) и (7) имеем

$$\tilde{X} = X(\tau) = 5\tau + 6 = 5(-t + 1) + 6 = 2t + 4,$$
$$\tilde{Y} = Y(\tau) = 2\tau + 4 = 2(-t + 1) + 4 = 5t + 6.$$

Тогда согласно (2), (3) и с учетом

$$A = -(X + \tilde{X}) = -(6 + 4) = 4,$$

$$B = X\tilde{X} = (5t + 6)(2t + 4) \bmod (t^2 - t - 1) =$$
$$= (3t^2 - 3t + 3) \bmod (t^2 - t - 1) = 6$$

дивизор (1) суммы точек P и $\tilde{P}$ в форме Мамфорда определяется полиномами

$$a(x) = (x - 5t - 6)(x - 2t - 4) = x^2 + 4x + 6,$$

$$b(x) = (2t + 4)\frac{x - (2t + 4)}{(5t + 6) - (2t + 4)} +$$
$$+ (5t + 6)\frac{x - (5t + 6)}{(2t + 4) - (5t + 6)} = 6x + 3,$$

Решим теперь обратную задачу – по известному дивизору найдем координаты сопряженных точек P и $\tilde{P}$. В нашем примере согласно (8) $\Delta = A^2 - 4B = 6$ является квадратичным невычетом в поле F_7. В расширенном поле можно найти квадратичный вычет в форме $\sqrt{\Delta} = \alpha(t + \frac{a_1}{2})$. Из (10) имеем

$$\alpha^2 = \frac{4 * 6}{1 + 4} \bmod 7 = 2, \quad \alpha = 3.$$

Тогда в соответствии с (11)

$$X = \frac{-4 + 3(t - \frac{3}{2})}{2} \bmod 7 = \frac{-4 + 3(t - 4)}{2} \bmod 7 = 5t + 6,$$

$$\tilde{X} = \frac{-4 - 3(t - 4)}{2} \bmod 7 = 2t + 4.$$

С помощью (12) находим y-координаты сопряженных точек

$$Y = 6X + 3 = 2t + 4, \qquad \tilde{Y} = 6\tilde{X} + 3 = 5t + 6.$$

Как видим, обратные вычисления дают значения координат точек P и $\tilde{P}$.

При $c = 0$ и $e = 0$ в (4) координаты точек лежат в основном поле $\boldsymbol{F}_p$, при этом сопряженные точки совпадают $P = \tilde{P}$, а дивизор их суммы отвечает удвоению точки P. Кроме того, над основным полем $\boldsymbol{F}_p$ формируются элементы якобиана, представляющие всевозможные пары различных не противоположных точек $\boldsymbol{C}$, определенных над этим полем, а также дивизоры веса 1, представляющие каждую одну такую точку. Отсюда следует, что пара точек кривой $\boldsymbol{C}$ и элементы ее якобиана изоморфны лишь над расширением $\boldsymbol{F}_p^2$. Заметим, однако, что при больших значениях модуля p, характерных для криптографических приложений, число точек $\boldsymbol{C}$ над расширением приблизительно в p раз преобладает над числом точек кривой, определенных над основным полем $\boldsymbol{F}_p$. Это значит, что и элементы якобиана кривой в основном формируются на основе пар точек над расширением $\boldsymbol{F}_p^2$.

ЗАКЛЮЧЕНИЕ

Для записи элемента якобиана гиперэллиптической кривой второго рода в виде полиномов $a(x)$ и $b(x)$ требуется 4 параметра A, B, G, $H \in \boldsymbol{F}_p$ (см. (2),(3)) общей длиной 4log$p$. Такой же размер имеет информация о двух координатах (X, Y) точки эллиптической кривой приблизительно того же порядка, что и у якобиана ГЭК-2. Представление дивизора с помощью одной точки из пары P, $\tilde{P}$ не дает выигрыша в памяти, так как координаты точки над расширением $\boldsymbol{F}_p^2$ опять имеют общий размер 4log p.

Для гиперэллиптической кривой третьего рода дивизор может состоять из трех, двух или одной точки. Приведенные выше аналитические соотношения в этом случае уже не работают. Для представления элемента якобиана необходимо хранить уже 6 параметров. Но при этом надо учитывать, что сами параметры имеют меньшую длину.

В общем случае, для гиперэллиптической кривой рода g в дивизор может входить максимум g точек. Для хранения одного элемента необходимо выделить память $2g \log p$ бит. С учетом того, что при сохранении одинакового уровня стойкости размер основного поля можно уменьшить пропорционально роду кривой, объем требуемой памяти приблизительно равен $2g\ (\log n)/g = 2 \log n$, где n – порядок якобиана. Ясно, что он не зависит от рода кривой, а определяется только выбранным уровнем стойкости.

Сократить объем требуемой памяти можно в том случае, если использовать дивизор веса 1 (для одной точки над полем $\boldsymbol{F}_p$), например, в качестве генератора якобиана.

Литература.

[1] *Menezes A.* An Elementary Introduction to Hyperelliptic Curves [Электронный ресурс] / Menezes A., Wu Y., Zuccherato R. : Published as Technical Report CORR 96-19 Department of C&O University of Waterloo : Ontario : Canada,– 1996.- P. 1-35. – Режим доступа: www.cacr.math.uwaterloo.ca/techreports/1997/corr96-19.ps.

[2] *Мамфорд Д.* Лекции о тэта-функциях / Д. Мамфорд. – М.: Мир. –1988. – 448 с.

[3] *Cantor D.G.* Computing in the Jacobian of a hyperelliptic curve / D.G. Cantor // Math. Comp. 48, 177. – 1987. – P. 95-101.

[4] *Wollinger T.* Fast explicit formulae for genus 2 hyperelliptic curves using projective coordinates (Updated) [Электронный ресурс] / T. Wollinger, V. Kovtun // Cryptology ePrint Archive, Report 2008/056. – 2003. – Режим доступа: http://eprint.iacr.org/2008/056.pdf.

[5] *Wollinger T.* Software and Hardware Implementation of Hyperelliptic Curve Cryptosystem : Dissertation for the Degree of Doctor-Ingenious / T. Wollinger. – Bochum. – Germany, – 2004. – 201 p.

Поступила в редколлегию 30.06.2010.

Бессалов Анатолий Владимирович, доктор технических наук, профессор, Военный институт телекоммуникаций и информатизации Национального технического университета Украины “Киевский политехнический институт”, профессор кафедры № 12, г. Киев. Область научных интересов: защита информации, криптография с открытыми ключами.

Неласая Анна Викторовна, старший преподаватель кафедры программных средств Запорожского национального технического университета. Область научных интересов: криптография на эллиптических кривых и гиперэллиптических кривых.

УДК 003.26

Ізоморфізм дивізорів та пар точок гіпереліптичної кривої роду два / А.В. Бессалов, Г.В. Неласа // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 418-420.

Розглядається питання представлення дивізора гіпереліптичної кривої точками в розширенні основного поля. Розкривається зв’язок між точками, що утворюють дивізор, для гіпереліптичної кривої другого роду.

Ключові слова: гіпереліптична крива, род кривої, дивізор, форма Мамфорда, ізоморфізм.

Бібліогр.: 05 найм.

UDC 003.26

Isomorphism of divisors and pair of points of genus two hyperelliptic curve / A.V. Bessalov, G.V. Nelasaya // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 418-420.

The question of representating a hyperelliptic curve divisor through points in extension of a base field is discussed. The relation between a divisor’s points for a genus two hyperelliptic curve is shown.

Key words: hyperelliptic curve, genus of a curve, divisor, Mumford form, isomorphism.

Ref.: 05 items.

МЕТОДЫ И СРЕДСТВА АНАЛИЗА И ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

УДК 629.735

ОЦЕНКА ГАРАНТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ФУНКЦИОНАЛЬНО-ЛИНГВИСТИЧЕСКОГО ПОДХОДА

А.В. ПОТИЙ, Д.С. КОМИН

Приводятся результаты онтологического анализа предметной области оценивания гарантий информационной безопасности. Предлагается подход к оцениванию уровня гарантий информационной безопасности, основанный на функциональном моделировании процесса оценки и введении лингвистических переменных, который направлен на выполнение требований глубины и строгости, предъявляемые к процессу оценки и требований объективности, повторяемости, воспроизводимости, беспристрастности и сопоставленности, предъявляемым к результатам оценки.

Ключевые слова: гарантии, уровень безопасности, онтологическое моделирование, оценивание.

ВВЕДЕНИЕ

Методологической основой современных технологий проектирования защищенных систем информационных технологий (ИТ-систем) и комплексных систем защиты информации (КСЗИ) являются международный стандарт ISO/IEC 15408 [1,2] и национальный нормативный документ НД ТЗИ 2.5-004-09 [3]. Эти документы предполагают выдвижение функциональных требований безопасности и требований гарантий, которые в ходе проектирования подлежат оцениванию на предмет их выполнения. Многолетний опыт применения этих нормативных документов сделали особенно актуальными задачи обеспечения и оценки гарантий безопасности (уровня доверия).

В общей проблеме обеспечения гарантий безопасности основополагающая роль принадлежит научно-теоретическому аспекту. В рамках данного аспекта можно выделить следующие разделы:

– терминология;

– стандартизация в сфере обеспечения гарантий безопасности;

– критерии оценки гарантий безопасности;

– способы определения (выбора) и обоснования требований и уровня гарантий;

– методы оценки уровня гарантий безопасности;

– модели процессов обеспечения гарантий безопасности;

– методы анализа уровня гарантий в ходе эксплуатации КСЗИ.

Терминология является инструментом взаимодействия и необходимым условием единства подходов к решению различных задач обеспечения гарантий. Активно развивается стандартизация в данной сфере, о чем свидетельствует разработка проектов стандартов НД ТЗИ 2.7-010-09 [4], ISO/IEC 18045 [5]. При определении и обосновании требований и уровня гарантий в основном применяются методы системного анализа (эвристические методы, методы экспертной оценка и т.д.). Оценка уровня гарантий сегодня осуществляется с использованием неформальных подходов.

Степень доверия к результатам оценивания (в любой сфере) определяется качеством и количеством усилий и ресурсов, затраченных на его проведение. Уровень оценки характеризуется широтой, т.е. степенью охвата элементов объекта оценивания, глубиной, т.е. детальностью рассматриваемых материалов об объекте оценивания и строгостью, т.е. уровнем формализации применяемых методов оценивания и качеством инструментальных средств оценки [6].

На сегодняшний день можно с уверенностью говорить, что как на национальном, так и на международном уровне, отсутствует какой-либо цельный научно-методический аппарат оценки гарантий безопасности. В настоящее время формируются основные принципы и подходы к решению этой задачи, о чем свидетельствует активная работа над проектами международных стандартов [7].

Все выше изложенное говорит о том, что создание формального научно-методического аппарата оценки гарантий безопасности, разработка методов оценки уровня гарантий, которые способны обеспечить строгость оценки и лягут в основу разработки инструментальных средств оценки является актуальной научно-технической задачей в сфере защиты информации.

В данной работе изложены результаты системно-онтологического анализа предметной области оценивания гарантий безопасности, который проводился с целью уточнения основных понятий в данной предметной области, и предлагается функционально-лингвистический подход к оценке гарантий безопасности, базирующийся на функциональном моделировании процесса

оценивания и применении лингвистических переменных для формализации записи качественных свойств объекта оценки (ОО).

1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ ОБЕСПЕЧЕНИЯ ГАРАНТИЙ БЕЗОПАСНОСТИ

В исторической ретроспективе требования гарантий безопасности были впервые закреплены в международном стандарте ISO/IEC 7498-2 [8]. В данном стандарте вводится общий механизм безопасности как «доверительная функциональность», под которой понимается совокупность рекомендаций и способов, реализуемых для обеспечения гарантий правильной и надлежащей работы других механизмов безопасности.

Позже, в документе NIST SP 800-30 [9], вводится базовая техническая модель защиты информации, в основу которой заложены пять основных целевых задач обеспечения безопасности информации, а именно – обеспечение конфиденциальности данных и системной информации, целостности данных и системы, доступности (системы, данных, ресурсов), наблюдаемости и гарантий безопасности. Именно в этом документе нормативно закрепляется понятие гарантий (assurance), под которым понимают обеспечение того, что перечисленные выше задачи будут адекватно удовлетворены. Это основа уверенности в том, что принятые меры защиты как технического, так и организационного характера реализованы корректно. Гарантированность – существенное требование, без которого реализация всех остальных требований безопасности бессмысленна [9].

Окончательно необходимость и обязательность выдвижения и обеспечения требований гарантий были закреплены в международном стандарте ISO/IEC 15408. Согласно [1, 2] требования безопасности должны включать функциональные требования безопасности и требования гарантий (доверия).

Функциональные требования безопасности определяют требования к функциям ИТ-системы, реализующим их механизмам и средствам защиты, которые непосредственно предназначены для обеспечения безопасности и определяют предусмотренный режим безопасности. К функциональным требованиям относятся, в частности, требования идентификации, аутентификации, аудита безопасности и др.

Требования гарантий (доверия) это требования, выполнение которых дает основание для уверенности в том, что ИТ-система обеспечивает достижение поставленных целей безопасности. Требования гарантий (доверия) включают совокупность требований к необходимым действиям разработчика ИТ-системы, к предоставлению соответствующих свидетельств обеспечения требуемого уровня безопасности и к действиям при оценке безопасности ИТ-системы. В их состав входят требования, например, к разработке, поддержке жизненного цикла, тестированию и др.

Тем не менее, до настоящего времени в среде специалистов еще есть определенная несогласованность и как переводить англоязычный термин *assurance*, и что понимать под ним. В различных документах, научной литературе предлагаются различные переводы и определения этого термина. Термин *assurance* переводят и как доверие (российская нормативная база) и как гарантии (украинская нормативная база), и определяют его, например, как основание для уверенности в том, что сущность отвечает своим целям безопасности [1]; основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности [2]; выполнение соответствующих действий или процессов для предоставления уверенности в том, что объект оценки будет удовлетворять своим целям безопасности [7]; совокупность требований (шкала оценок) для определения меры уверенности, что компьютерная системы корректно реализует политику безопасности [10]; мера уверенности в том, что информационно-коммуникационная система корректно реализует политику безопасности [11].

Авторами был проведен анализ понятий «гарантии» и «доверие», на основе которого сделаны следующие выводы.

Российские специалисты при переводе международного стандарта термин *assurance* перевели как *доверие*. Обосновывают это тем, что использование термина, однокоренного слову «гарантия», для перевода термина *assurance,* неприемлемо ввиду возможности его интерпретации в юридическом смысле [6]. В этом есть определенный смысл, но использование слова «доверие» не менее неподходящее, чем использования слова «гарантии».

В табл. 1 представлены возможные толкования термина «доверие», а в табл. 2 толкования термина «гарантии».

Исходя из определений термина *доверие*, которые были рассмотрены авторами, можно сделать вывод, что *доверие* это, прежде всего психологическое состояние субъекта, в силу которого субъект полагается на чужое мнение. По большей части это относится к эмоциональной, т.е. плохо рационализируемой сфере психики. Сам же термин *assurance* включает в себя больше технический аспект и отображает меры, которые должны быть приняты на всех этапах жизненного цикла ИТ-системы для обеспечения уверенности в выполнении предъявляемых функциональных требований. Поэтому не совсем верно характеризовать какие-либо меры термином доверие, поскольку термин имеет психологическое весьма субъективное значение. В какой-то степени можно говорить о доверии к предпринимаемым контрмерам, но о том, что доверие является характеристикой этих контрмер – говорить сложно, поскольку доверием можно характеризовать лишь психологическое состояние человека.

В украинской терминологии в области защиты информации [3, 11] предлагается использова-

Таблица 1

Толкования термина «доверие»

Уверенность в чьей-нибудь добросовестности, искренности, в правильности чего-нибудь.	Словарь Ожегова
Убежденность в честности, добросовестности, искренности кого-либо, чего-либо, в правильности чего-либо и основанное на этом отношение к кому-либо, чему-либо	http://www.rulib.info/
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 Доверие, в огромной своей части, относится к эмоциональной, т. е. плохо рационализируемой сфере психики. Оно способно порождать многие другие чувства (от любви до ненависти), состояния (от комфорта до стресса и фрустрации), социальные установки (от приятия до отторжения). Доверие по отношению к личности играет формообразующую роль.	Большой психологический словарь. Сост. Мещеряков Б., Зинченко В.
Убежденность в чьей-нибудь честности, порядочности; вера в искренность и добросовестность кого-нибудь	Толковый словарь русского языка Ушакова
Доверие — установка личности, представляющая безусловную веру, а иногда и заменяющая ее. Доверие проявляется в специфическом отношении субъекта к определенным объектам, связанным с ситуативной, актуальной значимостью и априорной надежностью (безопасностью) объекта для субъекта	Социальная психология. Словарь
Индикатор доверия – мера доверия инвестора к экономике и рынку ценных бумаг. В техническом анализе низкий или снижающийся уровень доверия рассматривается как понижательный знак.	Словарь по экономике и финансам
Пять характеристик доверия – характеристики, используемые для формирования мнения о кредитоспособности клиента: характер, функции, капитал, обеспечение и условия	Словарь по экономике и финансам
Чувство или убеждение, что такому-то лицу, обстоятельству или надежде можно доверять, верить; вера в надежность кого, чего	Толковый словарь живого великорусского языка Владимира Даля
Возникающее у членов сообщества ожидание того, что другие его члены будут вести себя более или менее предсказуемо, честно и с вниманием к нуждам окружающих, в согласии с некоторыми общими нормами	Азбука социального психолога-практика

Таблица 2

Толкования термина «гарантии»

Средства, способы и условия, с помощью которых обеспечивается осуществление предоставленных работникам прав в области социально – трудовых отношений.	Словарь «Бухгалтерский учет, налоги, хозяйственное право»
В гражданском праве, предусмотренное законом или договором обязательство, в силу которого какое-либо лицо (физическое или юридическое) отвечает перед кредиторами полностью или частично в случае неисполнения или ненадлежащего исполнения обязательства должником.	Большая советская энциклопедия
Ручательство, поручительство, порука, обеспеченье, залог, ответ (с ответом), заверение, заверка, безопаска, обезопаска, безопасенье, страх	Толковый словарь живого великорусского языка Владимира Даля
Поручительство за выполнение определенным лицом денежных или вещественных обязательств, форма ответственности за выполнение принятых обязательств. Гарантом исполнения обязательств договора могут быть как участники сделки, так и третье лицо, принимающее на себя ответственность	Современный экономический словарь
1) в гражданском праве предусмотренное законом или договором обязательство, в силу которого какое-либо лицо (физическое или юридическое) отвечает перед кредиторами полностью или частично при неисполнении или ненадлежащем исполнении обязательства должником; 2) установленное законом обязательство продавца отвечать за материальные недостатки товара в течение определенного срока	Большой юридический словарь
Гарантии – в торговле машинами и оборудованием – дополнительный раздел договора, в котором: - продавец принимает на себя ответственность за качество товара в течение определенного срока; – определяются: объем предоставляемой продавцом гарантии, гарантийный срок, обязанности продавца в случае обнаружения дефектного товара или несоответствия его договору.	Словарь по экономике и финансам
Государственная гарантия – способ обеспечения гражданско-правовых обязательств, в силу которого субъект (гарант) дает письменное обязательство отвечать за исполнение лицом, которому дается гарантия, обязательства перед третьими лицами полностью или частично.	Словарь по экономике и финансам
Гарантия безопасности – вероятность неразорения страховщика, вероятность превышения суммы нетто-премий над суммой выплат.	Словарь по экономике и финансам

ние термина *гарантии*, и соответствующие ему требования называют требованиями гарантий. С одной стороны нельзя не отрицать, что использование этого термина имеет ограничение из-за возможности его трактовки в юридическом смысле, поскольку ни международные, ни отечественные стандарты не предполагают каких-либо юридических обязательств ни разработчика, ни владельца ИТ-продукта относительно выполнения этих требований. Однако анализ определений данного термина в различных сферах деятельности позволяет говорить, что *гарантии* это не только юридические обязательства, но и средства, способы, условия и заверения выполнения чего-либо. Поэтому если не учитывать юридической составляющей данного понятия, то использование данного термина, на наш взгляд, более приемлемо при описании, характеристике и оценке требований безопасности.

Толкование термина *assurance* в английском языке означает намерение вселить уверенность, обещание, залог, поручительство, гарантии, страхование, свободу от сомнений. А антонимом в английском языке данному слову является слово *uncertainty* – неопределенность. Поэтому использование термина *гарантии* более адекватно английскому термину *assurance,* чем *доверие*. Кстати, ни один англо-русский словарь не дает перевода слова *assurance,* как доверие, а переводится как уверение, гарантия, заверение, уверенность, убежденность, страхование.

Таким образом, в данной работе и далее при исследовании предметной области оценки информационной безопасности мы будем использовать термин *гарантии*, как более подходящий по смыслу, значению и адекватности английскому термину *assurance*.

Исходя из всего вышесказанного, можно дать следующее определение:

Гарантии безопасности – это 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.

В основном объектом приложения требования гарантий являются организационные и технологические процессы проектирования, разработки и эксплуатации ИТ-систем, а задача эксперта подтвердить выполнение этих требований для формирования уверенности потребителя (или самого же разработчика) в заявленном уровне информационной безопасности.

2. ОНТОЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ ГАРАНТИЙ БЕЗОПАСНОСТИ

2.1. Задача онтологического анализа предметной области

Анализ предметной области представляет особый вид научной деятельности, в результате которого строится интерпретационная модель предметных знаний (в широком смысле). В процессе анализа последние делятся на инвариантные и прагматичные знания, концептуальные составляющие которых представляют онтологические знания предметной области [12]. Новым направлением в области средств и методов системного анализа предметной области является системно-онтологический анализ. Центральной идеей системно-онтологического подхода является разработка онтологической системы (ОнС), которая описывается выражением (1) и представляет онтологию предметной области (ПдО), состоящую из онтологии объектов, онтологии процессов и онтологии задач [12]:

$$\text{ОнС} = \{\text{О}^{\text{ПдО}}(\text{О}^{\text{О}}, \text{О}^{\text{П}}), \text{О}^{\text{З}}\}, \quad (1)$$

где $\text{О}^{\text{О}}$ – онтология множества объектов (понятий, концептов) ПдО, рассматриваемая как иерархическая структура классов, подклассов и элементов классов; $\text{О}^{\text{П}}$ – онтология множества процессов ПдО, рассматриваемая как иерархическая структура процессов, подпроцессов, действий и операций; $\text{О}^{\text{З}}$ – онтология совокупности задач, которые могут быть поставлены и решены в ПдО и рассматриваемая как иерархическая структура задач, подзадач, процедур и операторов.

Под онтологией множества понятий понимается кортеж четырех множеств [12]:

$$\text{О}^{\text{О}} = <X, R, F, A(D, Rs)>, \quad (2)$$

где $X = \{x_1, x_2, ..., x_i, ..., x_n\}$, $i = \overline{1,n}$, $n = Card\, X$ – конечное множество концептов (понятий) заданной предметной области; $R = \{r_1, r_2, ..., r_k, ..., r_m\}$, $R: x_1 \times x_1 \times x_2 \times ... \times x_n$, $k = \overline{1,m}$, $m = Card\, R$ – конечное множество семантически значимых отношений между концептами предметной области; $F = X \times R$ – конечное множество функций интерпретации, заданных на концептах и/или отношениях; A – конечное множество аксиом, которые используются для записи всегда истинных высказываний (определений и ограничений).

Первичный анализ нормативных документов [1-5, 7-10], научно-технической литературы [6, 11] позволил выделить следующие объекты онтологического моделирования:

– термины-объекты: гарантии, уровень гарантий, критерии гарантий, уверенность, программа оценивания, методика оценивания, объект оценки, безопасность информации, меры обеспечения безопасности, уязвимость, угроза, риск, вердикт, общий вердикт;

– термины-процессы: оценивание, аккредитация, сертификация, действие, шаг, проверка, исследование, верификация.

2.2. Онтологические модели предметной области гарантий безопасности

На рис. 1 показан контекст безопасности ИТ-продукта согласно международному стандарту ISO/IEC 15408. ИТ-безопасность связана с защитой активов от угроз. Во внимание следует принимать все разновидности угроз, но в сфере

безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека (умышленные и неумышленные). За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца.

К специфическим нарушениям безопасности обычно относят (но не обязательно ими ограничиваются): наносящее ущерб раскрытие актива несанкционированным получателем (потеря конфиденциальности), ущерб активу вследствие несанкционированной модификации (потеря целостности) или несанкционированное нарушение доступа к активу (потеря доступности).

Владельцы активов будут анализировать возможные угрозы, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются риски. Анализ может помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня.

Контрмеры предпринимают для уменьшения уязвимостей и корректного выполнения политики безопасности. Но и после введения этих контрмер могут сохраняться остаточные риски для активов. Владельцы будут стремиться минимизировать эти риски, задавая дополнительные ограничения.

Прежде чем подвергнуть активы опасности воздействия выявленных угроз, их владельцам необходимо убедиться, что предпринятые контрмеры обеспечат адекватное противостояние этим угрозам. Сами владельцы активов не всегда в состоянии судить обо всех аспектах предпринимаемых контрмер и поэтому могут потребовать их оценку. Результатом такой оценки является заключение о степени доверия контрмерам по уменьшению рисков для защищаемых активов. В этом заключении устанавливается уровень гарантий как результат применения контрмер.

Гарантии являются той характеристикой контрмер, которая дает основание для уверенности в их надлежащем действии. Заключение о результатах оценки может быть использовано владельцем активов при принятии решения о приемлемости риска для активов, создаваемого угрозами. Рис. 2 иллюстрирует эту взаимосвязь. Поскольку ответственность за активы несут их владельцы, то они должны иметь возможность отстаивать принятое решение о приемлемости риска для активов, создаваемого угрозами. Для этого требуется, чтобы результаты оценки были правомерными. Следовательно, оценка должна приводить к объективным и повторяемым результатам, что позволит использовать их в качестве свидетельства.

Онтологическая модель, описывающая предметную область понятий «*уверенность*» и «*гарантии*», представлена на рисунке 3. Мерой уверенности в том, что в ИТ-продукте обеспечивается требуемый уровень защиты информации, в том, что КСЗИ решает задачи защиты информации является *уровень гарантий (assurance level)*. В свою очередь *уверенность (confidence)* есть вера в то, что ИТ-продукт (т.е. объект оценки безопасности) будет выполнять задачи защиты соответствующим образом (правда не в одном стандарте пока не определено, что значит соответствующим образом). Уровень гарантий – это совокупность *требова-*

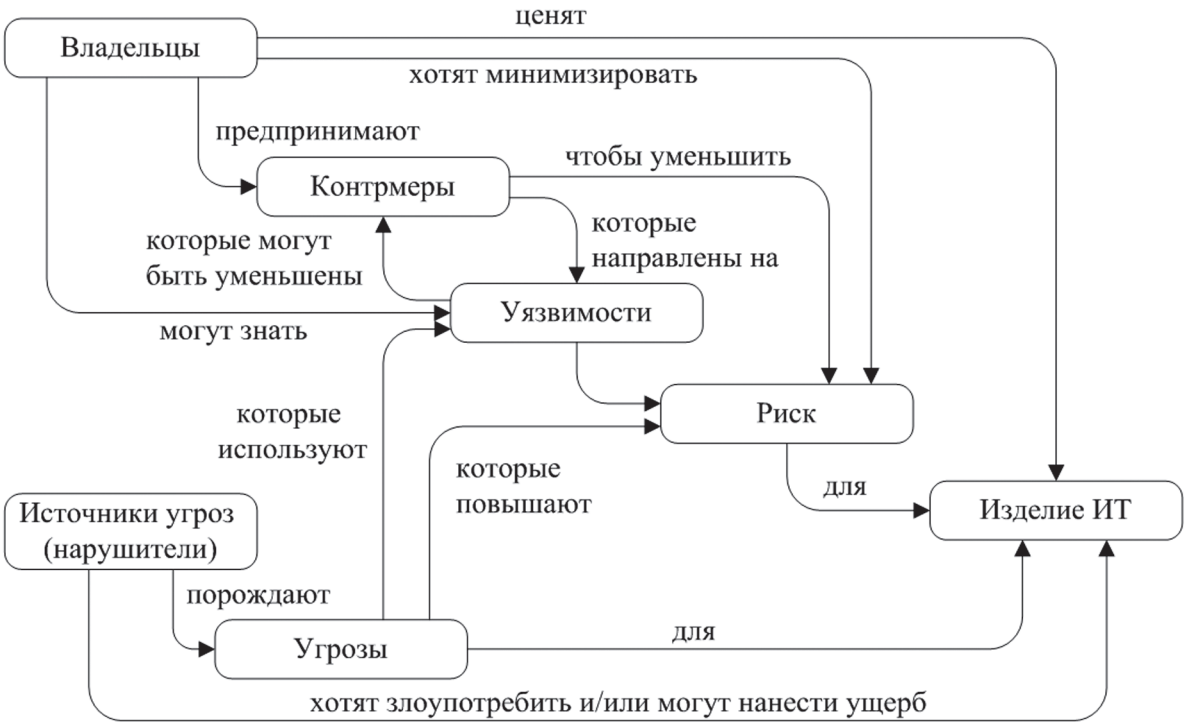


Рис. 1. Взаимосвязь основных понятий в сфере ИТ-безопасности [1]

ний гарантий (assurance requirements), выполнение которых характеризует корректность реализации функциональных требований безопасности, способность ИТ-продукта противостоять угрозам безопасности и обеспечивать достижение (и сохранения) требуемого уровня защищенности информации в системе. Требования гарантий выдвигаются к *объекту оценки (deliverable),* в качестве которого выступает средство технической защиты информации от несанкционированного доступа (НСД), защищенный от НСД компонент вычислительной системы или комплекс средств защиты (КСЗ) комплексной системы защиты информации (КСЗИ).

В отношении объекта оценки осуществляется процесс *оценивания (evaluation)*, с целью определения выполнения требований гарантий (рис. 4). Процесс оценивания осуществляется на основе *программы* и *методики* оценивания, в рамках сертификации объекта оценки и в соответствии *критериями* оценивания.

Программа оценивания (evaluation program) – документированная совокупность требований гарантий, которые подвергаются проверке в процессе оценивания объекта оценки. *Методика оценивания (evaluation methodic)* – определенные (установленные) способы проведения оценки требований гарантий. *Сертификация (certification)* – процедура, при которой устанавливается уровень гарантий. Сертификация должна проводиться третьими лицами (независимыми экспертами) с целью предоставления окончательного заключения. В процесс оценивания вовлечены субъекты оценивания – эксперт, орган оценки, владелец ИТ-продукта, разработчик ИТ-продукта. *Эксперт (оценщик)* – физическое лицо, обладающее соответствующими компетенциями, достаточными для проведения оценивания гарантий безопасности. Учитывая, что есть несколько стадий жизненного цикла объекта оценки, может быть и несколько соответствующих специалистов для оценивания гарантий на том или ином этапе жизненного цикла. *Орган оценки гарантий (assurance authority)* – организация, обладающая соответствующими полномочиями для принятия (утверждения) решений, связанных с оцениванием уровня гарантий и выдачи соответствующих документов (сертификатов).

Критерии оценивания (evaluation criteria) – формальные или неформальные правила, на основе которых принимается решение относительно выполнения требований гарантий. Выходом процесса оценивания является *результат оценивания гарантий (assurance result)* – задокументированная количественная или качественная ха-

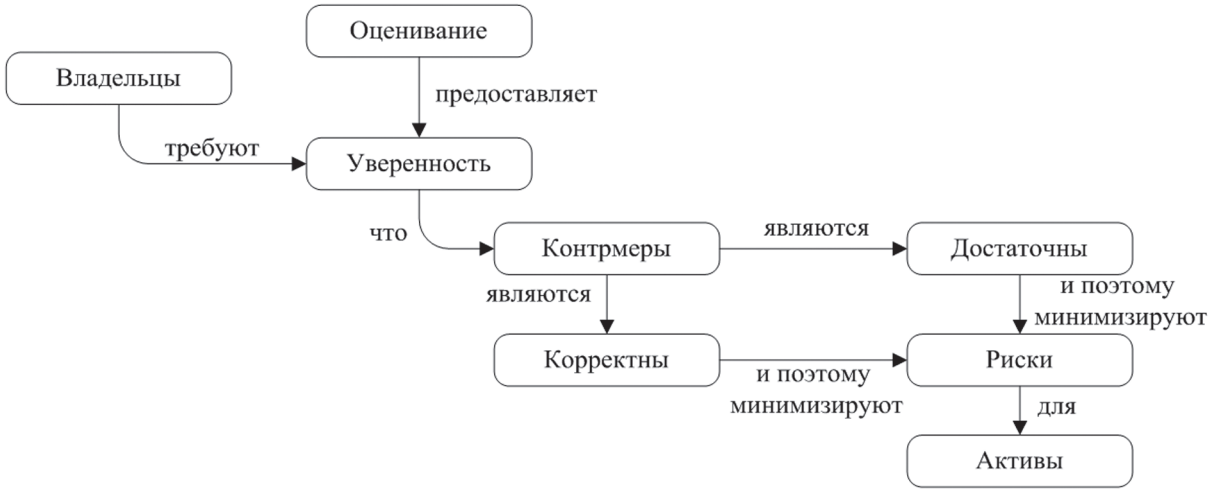


Рис. 2. Понятие оценивания и его значение для владельцев [13]

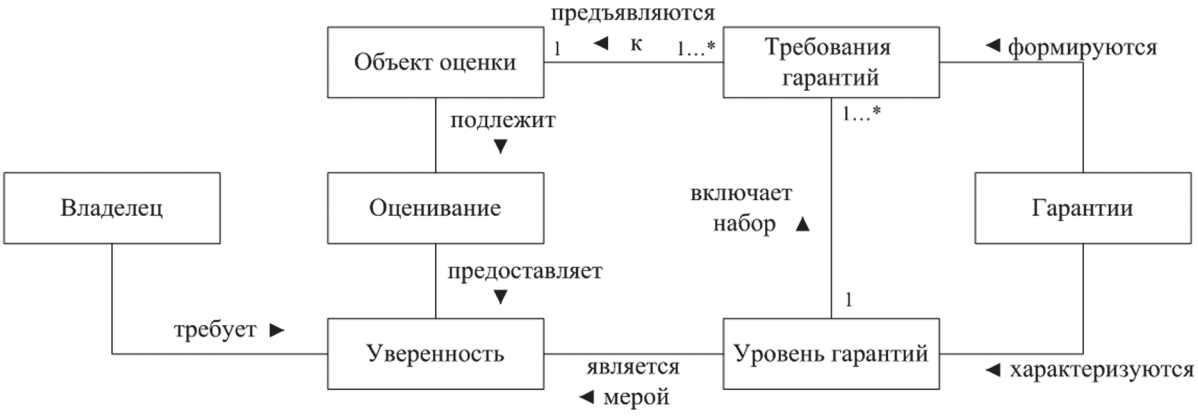


Рис. 3. Онтологическая модель понятий «уверенность» и «гарантии»

рактеристика объекта оценивания. К результатам оценивания выдвигаются требования объективности, повторяемости, воспроизводимости, беспристрастности и сопоставимости.

Объективность – свойство, которое предполагает, что результаты оценки гарантий безопасности должны быть фактическими, т.е. не подверженными влиянию чувств или мнений эксперта (оценщика). *Повторяемость* – свойство, которое обеспечивает идентичность результатов оценивания при повторной оценке одного и того же ОО, которая проводится по той же программе и методике оценке гарантий безопасности и тем же экспертом (оценщиком). *Воспроизводимость* – свойство, которое обеспечивает идентичность результатов оценивания при повторной оценке одного и того же ОО, которая проводится по той же программе и методике оценке гарантий безопасности различными экспертами (оценщиками). *Беспристрастность* – свойство, которое предполагает, что оценка гарантий безопасности не должна быть предубежденной по отношению к любому специфическому результату оценивания. *Сопоставимость* – свойство, которое обеспечивает сравнимость результатов оценивания, полученных при оценке одного и того же ОО по различным программам и методикам оценивания различными (или одним и тем же) экспертами.

3. ОБЩИЙ ПОДХОД К ОЦЕНКЕ УРОВНЯ ГАРАНТИЙ

Предлагаемый подход к оценке уровня гарантий направлен на выполнение требований глубины и строгости оценивания. Глубина оценивания гарантий определяется степенью детальности рассматриваемых материалов об объекте оценивания. Строгость оценивания определяется уровнем формализации применяемых методов оценивания и качеством инструментальных средств оценки [6].

Оценке подвергается объект оценки (ОО), под которым понимается набор программных, программно-аппаратных и/или аппаратных средств сопровождаемых руководствами [13]. ОО может быть ИТ-продукт, часть ИТ-продукта или набор ИТ-продуктов. Отдельные части ОО называют свидетельствами. Методология [5] предполагает оценивание именно отдельных свидетельств, по результатам оценки которых и формируется соответствующее мнение (вердикт) и общий вывод о соответствии заявленному уровню гарантий.

На рис. 5 представлена общая схема, характеризующая функционально-лингвистический подход к оценке уровня гарантий безопасности. Подход направлен на исследование методологии оценивания, создание на ее основе формализированного аппарата для оценивания уровня гарантий и предполагает последовательное выполнение 6 этапов.

Глубина оценивания достигается путем анализа ОО, четкого определения множества свидетельств и однозначного выделения множества свойств ОО, подлежащих оценке. Для этого предлагается использовать процедуру декомпозиции.

Этап 1. В результате анализа и декомпозиции ОО формируется точное множество свидетельств

Рис. 4. Онтологическая модель «оценивания гарантий»

оценки. Количество уровней декомпозиции зависит от задач оценивания. Декомпозиция свойств может быть представлена в виде таксономии и в виде формальной записи отдельных множеств.

Рис. 5. Общий подход к оценке гарантий безопасности

Этап 2. На данном этапе выделяется множество свойств, подлежащих оцениванию. Определяются типы отношений на данном множестве свойств (отношения зависимости, отношения типа «часть-целое» и др.). Устанавливается соответствие между множеством свидетельств и множеством свойств. Выделяются подмножества свидетельств для оценки каждого отдельного свойства. Выделенные свойства классифицируются по сложности, оценивается сложность оценки свойства и определяются составные свойства.

Декомпозиция свойств в сочетании с четко определенными свидетельствами, и соответствующее представление результатов декомпозиции (например, в виде графов, матриц) позволяет убедительно продемонстрировать степень детализации ОО и даже дать количественную оценку глубины оценивания. Это позволит объективно судить о степени выполнения требования глубины оценивания. Степень декомпозиции, как ОО, так и оцениваемых свойств, соответствует уровню гарантий, на соответствие которому необходимо проверить ОО. Поэтому для каждого следующего уровня гарантий предыдущее множество свидетельств и свойств будет наращиваться, а как следствие, будет усложняться процедура оценивания и увеличиваться затраты ресурсов для ее проведения.

С целью обеспечения строгости оценивания в работе предлагается формализовать процесс оценивания. Поскольку методология оценивания гарантий, определенная стандартом ISO/IEC 18045 [4], имеет вид вербального описания процесса проведения оценивания (прежде всего как деятельности эксперта), то задачу формализации оценивания предлагается решить путем использования методологии функционального моделирования процессов [5-8]. Под *моделированием* будем понимать процесс создания точного, достаточного, лаконичного, удобного для восприятия и анализа описания процессов оценивания, как совокупности взаимодействующих компонент и взаимосвязей между ними. Результаты анализа описания процессов оценки в стандарте ISO/IEC 18045, особенности описания и представления результатов оценки показали, что для описания процесса оценивания целесообразно использовать функциональное моделирование в нотациях IDEF0 и IDEF3 [5-7]. Выбор методологии функционального моделирования IDEF0 обусловлен рядом существенных преимуществ:

– графическое и текстовое представление моделируемой деятельности;

– компактность;

– обмен информацией;

– функциональная декомпозиция;

– коммуникативность и ограничения сложности;

– строгость, точность, формализм и однозначность.

Этап 3. Выполняется построение моделей процесса оценивания гарантий в нотации IDEF0. Моделирование производится в соответствии с определенными на предыдущих шагах множеством свидетельств и множеством оцениваемых свойств. Множество свойств используется для определения названий блоков диаграмм. Выделенные подмножества свидетельств, необходимые для оценки отдельных свойств, обозначаются входными стрелками в блоки по оценке соответствующих свойств. Правильное использование семантики языка IDEF0 при моделировании позволяет однозначно описать для каждого шага оценивания: что оценивается (названия блоков), свидетельства оценки (входные дуги), на основании чего оценивается (дуги управления), кем оценивается (дуги механизмов) и результат оценивания (выходные дуги). В зависимости от сложности свойства, каждый блок диаграммы (шаг по оцениванию отдельного свойства) может быть декомпозирован в дочернюю диаграмму для описания множество оцениваемых подсвойств.

Одним из важных и труднодостижимых свойств является объективность результатов оценивания. Достижение требуемой степени объективности усложняется тем, что в большинстве случаев оценка свойств, характеризующих гарантии безопасности, осуществляется на основе субъективного мнения эксперта. В предлагаемом подходе для обеспечения объективности резуль-

татов оценки предлагается ограничить свободу выбора эксперта, как лица, принимающего решение. То есть эксперту предлагается осуществлять выбор (в частности давать оценку о степени проявления того или иного свойства) из заранее обоснованного и конечного множества альтернатив. Это достигается путем четкого и ясного описания оцениваемого свойства (характеристики) ОО и формального его представления в виде лингвистической переменной.

Этап 4. Для каждого оцениваемого свойства вводится лингвистическая переменная и определяются значения, которые она может принимать. Под ЛП будем понимать переменную, значением которой являются нечеткие подмножества, выраженные в форме слов или предложений на естественном или искусственном языке [14]. Формально ЛП задается кортежем <β, $T(\beta)$, G, M>, в котором β – название ЛП; $T(\beta)$ – терм-множество ЛП, элементами которого есть наименования нечетких переменных; G – синтаксическое правило, которое порождает названия нечетких переменных; M – синтаксическое правило, которое ставит в соответствие каждой нечеткой переменной γ нечеткое подмножество $\tilde{C}(\gamma)$. Нечеткой переменной называют кортеж <γ, X, $\tilde{C}(\gamma)$ >, где X – область определения нечеткой переменной, а нечеткое подмножество $\tilde{C}(\gamma)=\{\mu_{\tilde{C}(\gamma)}/x\}$. $\mu_{\tilde{C}(\gamma)}$ – функция принадлежности нечеткого подмножества $\tilde{C}(\gamma)$. Определение функций принадлежности нечетких подмножеств лингвистических переменных, носящих исключительно качественный характер, затруднительно, и решается путем постановки экспертизы и введением условных шкал.

Введение ЛП сопровождается лингвистической неопределенностью, которая связана с использованием естественного языка для описания задачи принятия решений. Эта неопределенность обусловливается необходимостью оперировать конечным числом слов и ограниченным числом структур фраз (предложений, абзацев, текстов) для описания бесконечного множества разнообразных ситуаций, возникающих в процессе принятия решений. Лингвистическая неопределенность порождается, с одной стороны, множественностью значений слов (понятий и отношений) языка, а с другой стороны, неоднозначностью смысла фраз [15].

Этап 5. Для каждой IDEF0 диаграммы строятся диаграммы потоков работ в нотации IDEF3. Такие диаграммы позволяют определить приоритетность выполнения шагов оценивания и наглядно отобразить порядок действий оценщика. Это достигается наличием в данной нотации, так называемых, перекрестков, которые и «направляют» эксперта по тому или иному потоку работ в зависимости от его предыдущего решения. Каждый блок диаграммы представляет собой отдельное действие оценщика. После каждого блока следует перекресток, выходные стрелки которого определяют следующий шаг оценивания. Выбор стрелки зависит от того, какое решение примет эксперт относительно степени проявления оцениваемого свойства. Количество стрелок (по сути вариантов выбора) зависит от количества значений, которые может принимать ЛП, описывающая оцениваемое свойство. Диаграммы позволяют определить точки, в которых эксперт должен принять решение и вынести вердикт относительно оценки того или иного свойства.

При построении IDEF3 диаграмм используются графы зависимостей свойств. Для определения приоритетности оценивания свойств их необходимо отранжировать. Одним из возможных вариантов ранжирования и постановки экспертизы является метод анализа иерархий [16]. Построение IDEF3 диаграмм способствует выполнению требования повторяемости и воспроизводимости результатов оценивания, т.к. для каждого шага оценивания определяется набор вариантов вердиктов. Выбор варианта вердикта зависит от того, какие значения принимают лингвистические переменные в ходе оценивания свойств (по сути это выбор эксперта относительно степени проявления свойства).

Этап 6. Исходя из множества значений, которые могут принимать лингвистические переменные, разрабатываются продукционные правила формирования промежуточных и окончательных вердиктов. Вердикты разрабатываются таким образом, чтобы в нем содержался общий вердикт и краткий отчет по каждому действию. Применение шаблонных вердиктов направлено на выполнение требования сопоставимости результатов оценивания.

4. ПРИМЕНЕНИЕ ПОДХОДА НА ПРИМЕРЕ ОЦЕНКИ ПО УРОВНЮ ГАРАНТИИ 1

Подход, представленный на рис. 5, был на практике применен для формального описания процесса оценивания на соответствие требованиям уровня гарантии 1.

1 этап. На данном этапе был проведен анализ требований гарантий, выдвигаемых при оценке на соответствие уровню гарантии 1. Это позволило выделить множество свидетельств, подлежащих оцениванию: S_{EAL1} = {задание по безопасности (ЗБ), функциональная спецификация (ФС), руководство администратора (РА), руководство пользователя (РП), процедуры установки, генерации и запуска (ПУГЗ), непосредственно объект оценки (ОО)}. Данное множество показывает первый уровень декомпозиции. Пример декомпозиции второго уровня можно привести на примере декомпозиции ЗБ на множество свидетельств, подлежащих оцениванию: $EAL1_{ZB}$ = {раздел «Описание ОО», раздел «Среда безопасности ОО», раздел «Введение ЗБ», раздел «Цели ЗБ», раздел «Цели безопасности», раздел «Утверждения о соответствии ПЗ», раздел «требования безопасности ИТ», раздел «Краткая спецификация ОО»}. Результаты декомпозиции могут быть представлены в виде таксономии (рис. 6).

2 этап. В ходе выполнения процедуры декомпозиции формируется множество свойств, присущих соответствующим свидетельствам, и выявляются отношения зависимости на множестве свойств. В частности для ПУГЗ установлено, что оценке подлежит *достаточность* документации, описывающей ПУГЗ, которая в свою очередь зависит, например, от *предоставления* ПУГЗ; при оценке РА оцениванию подлежит *достаточность* описания РА для безопасного администрирования ОО, которая зависит, например, от *полноты* описании параметров безопасности, контролируемых администратором. Выделяются сложные свойства, т.е. такие свойства, для оценки которых необходимо оценить несколько подсвойств. Так, для оценки *достаточности* документации, описывающей ПУГЗ, необходимо оценить множество подсвойств – SV_{dost} = {Предоставление; Полнота описания; Приведение}. Выявляются зависимости для каждого множества подсвойств. Выявленные в ходе анализа зависимости между свойствами предлагается представлять в виде онтологического графа зависимостей свойств в нотации IDEF5 [17].

Граф зависимостей свойств по оценке достаточности документации, описывающей ПУГЗ, представлен на рис. 7.

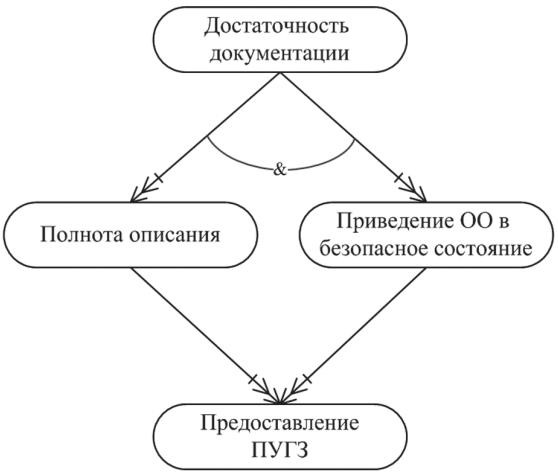


Рис. 7. Граф зависимостей свойств по оценке документации, описывающей ПУГЗ

Анализ показал, что на множестве свойств гарантий проявляются отношения типа «каузальная зависимость» и «экзистанциональная зависимость» (в данном примере только экзистанциональная). Свойство А является экзистанционально зависимым от свойства В, если существование свойства А зависит от существования свойства В. Свойство А является каузально зависимым от свойства В, если свойство А является результатом свойства В (свойство В является причиной или одной из причин существования свойства А) [17]. Учет свойств зависимости позволяет определить порядок их оценивания.

Декомпозиция позволяет определить, что для оценивания какого-либо свойства ОО может потребоваться одно или несколько свидетельств. Так, для оценки *достаточности* документации, описывающей ПУГЗ, необходимо проверить или исследовать множество свидетельств S_{dost} = {ПУГЗ; РА; ОО}.

Обобщенные результаты декомпозиции свидетельств и свойств с учетом выявленных зависимостей заносятся в таблицу соответствия свидетельств и свойств. Пример таблицы соответствия по оценке *достаточности* документации, описывающей ПУГЗ, представлен в табл. 3.

Таблица 3

Таблица соответствия свидетельств и свойств, по оценке достаточности документации, описывающей ПУГЗ

Достаточность документации, описывающей ПУГЗ			
SV_{dost} / S_{dost}	Предо-ставление	Полнота описания	Приведение ОО в безоп. сост.
ПУГЗ	1	1	1
РА	0	0	1
ОО	0	0	1

В таблицу соответствия в первой строке по горизонтали заносится множество свойств, которые необходимо оценить, а в первый столбец по вертикали – множество свидетельств, необходимых для оценки выделенного множества свойств. На пересечении строки и столбца ставится «1» тогда, когда свидетельству, записанному в соответствующей строке, присуще свойство соответс-

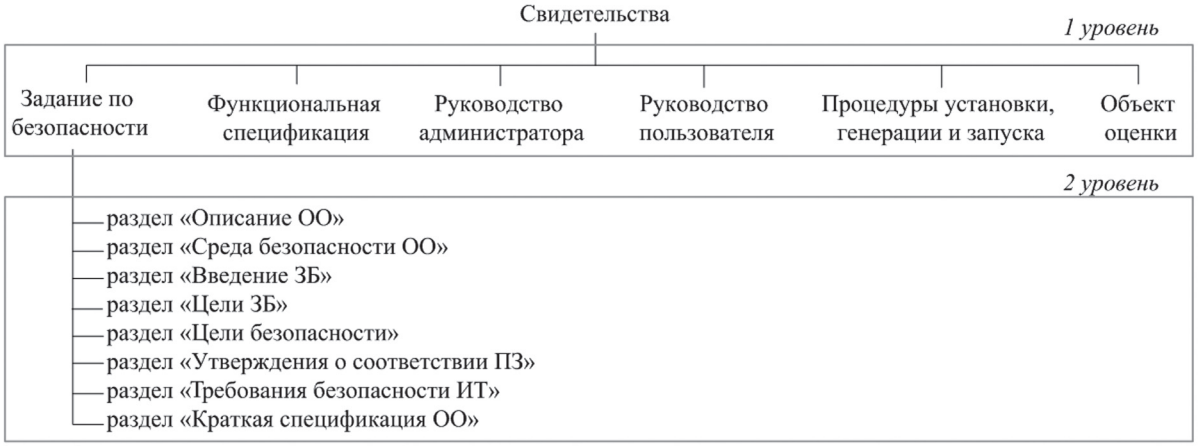


Рис. 6. Таксономия декомпозиции свидетельств

твующего столбца, или, иными словами, когда для оценки свойства, записанного в столбце, необходимо использовать свидетельство соответствующей строки. В ячейке таблицы записывается «0», если между свидетельством и свойством соответствующих столбца и строки нет взаимосвязи (соответствия).

Заполнение таблицы соответствия упорядочивает (систематизирует) знания об объекте оценки и позволяет уточнять характеристику оцениваемых свойств. Это, в конечном итоге, оказывает влияние на объективность и беспристрастность оценки свойств гарантий.

Так, из табл. 3 видно, что свойство «*приведение* ОО в безопасное состояние» присуще трем свидетельствам. Но учитывая особенности этих свидетельств, эксперту необходимо оценить различные аспекты проявления этого свойства. Так, свойство «*приведение* ОО в безопасное состояние», примененное к ОО, означает, что в ходе оценки эксперт должен проверить (исследовать), что реализованные в ОО процедуры (ПУГЗ)действительно переводят ОО в описанную безопасную конфигурацию (фокус на реализацию процедур в ОО). Относительно РА эксперт должен оценить, что точное следование инструкциям руководства и выполнение определенных в нем действий над ОО обеспечивают приведение ОО в безопасное состояние (т.е. фокус на описание процедур в руководстве). При оценке данного свойства для ПУГЗ фокус эксперта направлен на исследование корректности описания ПУГЗ и описания состояния ОО, реализуемое данными процедурами.

3 этап. На данном этапе осуществляется моделирование процесса оценивания. Моделирование осуществляется в соответствии с нотацией IDEF0. При моделировании используются результаты предыдущих этапов для определения названия блоков IDEF0-диаграмм, входных, выходных потоков, потоков управления. На рис. 8 представлен блок IDEF0 диаграммы по оценке ПУГЗ.

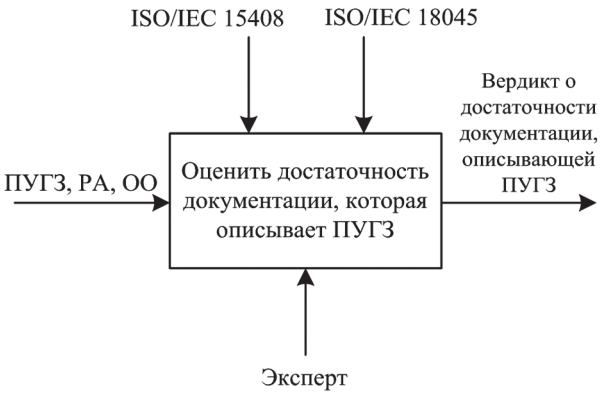


Рис. 8. Блок IDEF0 Диаграммы по оценке ПУГЗ

Названия блоков диаграмм точно определяют оцениваемое на данном шаге свойство. Входами блоков являются свидетельства, которые подлежат оцениванию, а выходом – вердикт об оценке оцениваемого свойства.

Представленный на рис. 8 блок диаграммы имеет однозначное толкование и в соответствии с нотацией читается так: «Эксперт должен оценить достаточность документации, которая описывает ПУГЗ. Используя в качестве свидетельств ПУГЗ, РА и ОО, и руководствуясь стандартами ISO/IEC 15408, ISO/IEC 18045, вынести вердикт о достаточности документации, описывающей ПУГЗ».

Используя данные декомпозиции свойства достаточности, блок диаграммы, представленный на рис. 8, декомпозируется в дочернюю диаграмму. На декомпозированной диаграмме каждое подсвойство отображается в отдельном блоке (рис. 9).

4 этап. На данном этапе для формализации записи вербально представленных свойств ОО, подлежащих оценке, вводится множество ЛП и определяются значения, которые они могут принимать.

Например, для оценки достаточности документации, описывающей ПУГЗ, была введена ЛП «*Достаточность*», которая может принимать множество значений: *Достаточность = {Достаточно, Вполне достаточно, Недостаточно}*.

5 этап. Построенные диаграммы оценивания гарантий в нотации IDEF0 дополняют диаграммы в нотации IDEF3.

На рис. 10 представлен результат моделирования процесса оценки достаточности документации, описывающей ПУГЗ в нотации IDEF3. Данная диаграмма отображает порядок действий оценщика. После каждого действия выходные стрелки соответствующего перекрестка показывают, какие значения может принять лингвистическая переменная. Так, при оценке полноты описания шагов безопасной установки, генерации и запуска ЛП «Полнота описания» может принимать три значения: {Описание полное, Описание вполне полное, Описание неполное}. В соответствии с этим, перекресток (на рис. 10 обозначен J2) имеет три выходные стрелки с аналогичными названиями.

IDEF3 диаграмма отображает зависимости свойств. Поэтому, для облегчения построения диаграмм, необходимо использовать результаты, полученные на этапе 2 (в частности, графы зависимостей свойств). Из диаграммы, представленной на рисунке 10, видно, что оценка *полноты* описания зависит от проверки *наличия* описания. Данная зависимость выражается в том, что оценка *полноты* описания не может начинаться до проверки *наличия* описания. Более того, если в результате проверки *наличия* описания эксперт определит, что *описание не представлено*, то, двигаясь по соответствующей стрелке, он выносит вердикт, минуя оценку других свойств. Возможность досрочного прекращения оценивания позволит сэкономить время и ресурсы при проведении оценивания.

6 этап. На данном этапе для каждой контрольной точки (перекрестка) IDEF3 диаграмм было сформировано множество шаблонов вердиктов

(вариантов выбора эксперта). Выбор одного из шаблонов зависит от значения, которое принимает ЛП при оценке текущего свойства. Для вынесения окончательных вердиктов были сформированы продукционные правила. Окончательный вердикт может быть либо положительным, либо отрицательным. Количество шаблонов окончательных вердиктов вытекает из количества стрелок, входящих в перекресток, предшествующий блоку вынесения вердикта (J5 на рисунке 10).

При оценке *достаточности* документации, описывающей ПУГЗ, может быть 6 вариантов вердиктов. Ниже приводятся набор данных вердиктов.

Вариант 1. *Достаточно = {Представлено, Полное, Приводит}.*

Представленная документация, в которой описываются ПУГЗ ОО, является достаточной для обеспечения ПУГЗ ОО, а ПГУЗ приводят к безопасной конфигурации ОО. Проверено, что в документации представлено описание ПУГЗ. Представленное описание является полным. В ходе исследования установлено, что ПУГЗ приводят к безопасной конфигурации ОО.

Вариант 2. *Недостаточно = {Представлено, Полное, Не приводит}.*

Представленная документация, в которой описываются процедуры безопасной установки, генерации и запуска объекта оценки, является недостаточной для обеспечения ПУГЗ ОО, а ПГУЗ не приводят к безопасной конфигурации ОО.

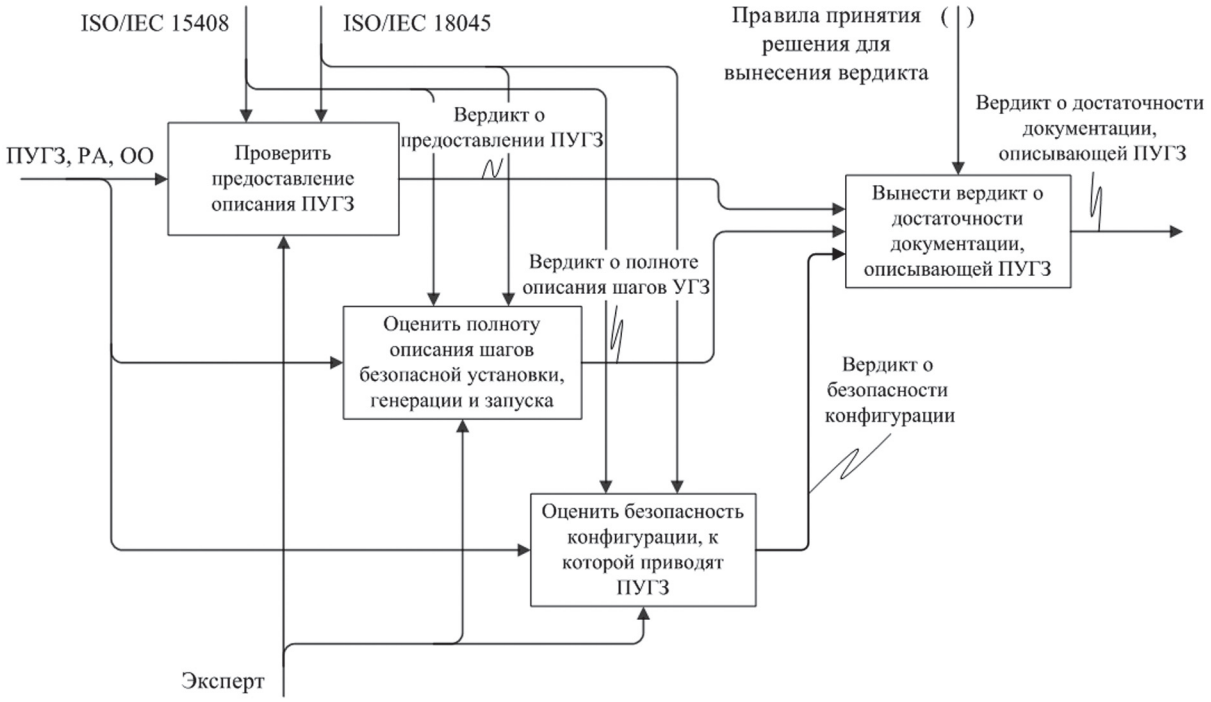


Рис. 9. Декомпозированная диаграмма по оценке достаточности ПУГЗ

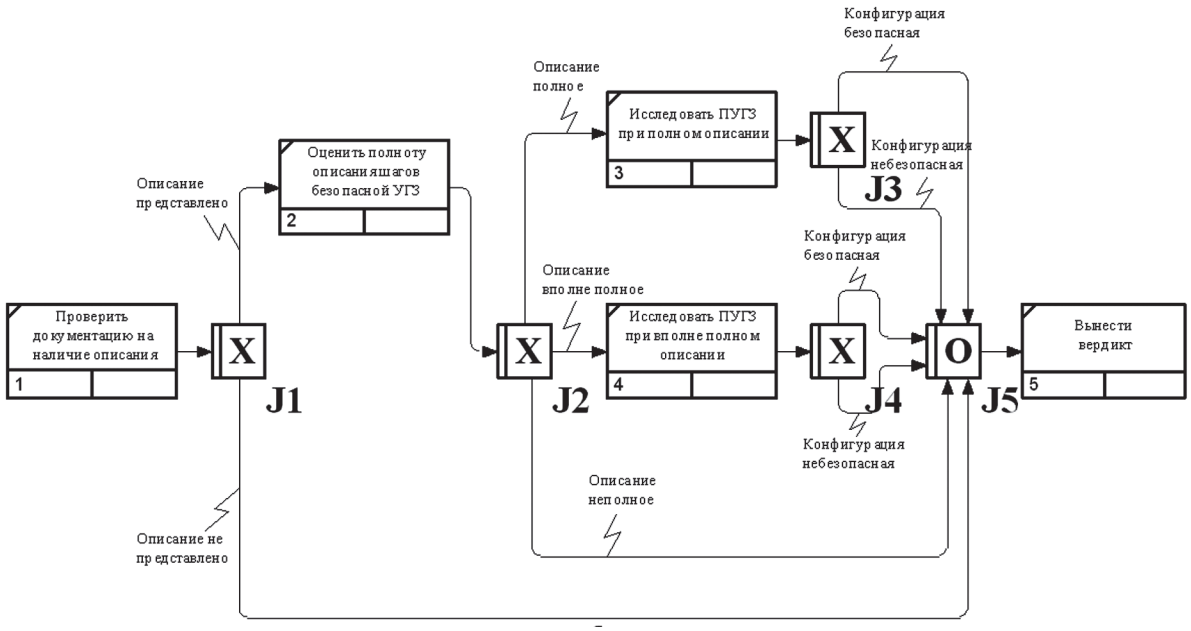


Рис. 10. IDEF3 диаграмма потоков работ по оценке достаточности документации, описывающей ПУГЗ

Проверено, что в документации представлено описание ПУГЗ. Представленное описание является полным. В ходе исследования установлено, что ПУГЗ не приводят к безопасной конфигурации ОО.

Вариант 3. *Вполне достаточно = {Представлено, Вполне полное, Приводит}.*

Представленная документация, в которой описываются процедуры безопасной установки, генерации и запуска объекта оценки, является вполне достаточной для обеспечения ПУГЗ ОО, а ПГУЗ приводят к безопасной конфигурации ОО.

Проверено, что в документации представлено описание ПУГЗ. Представленное описание является вполне полным. В ходе исследования установлено, что ПУГЗ приводят к безопасной конфигурации ОО.

Вариант 4. *Недостаточно = {Представлено, Вполне полное, Не приводит}*

Представленная документация, в которой описываются процедуры безопасной установки, генерации и запуска объекта оценки, является недостаточной для обеспечения ПУГЗ ОО, а ПГУЗ не приводят к безопасной конфигурации ОО.

Проверено, что в документации представлено описание ПУГЗ. Представленное описание является вполне полным. В ходе исследования установлено, что ПУГЗ не приводят к безопасной конфигурации ОО.

Вариант 5. *Недостаточно = {Представлено, Неполное}.*

Представленная документация, в которой описываются процедуры безопасной установки, генерации и запуска объекта оценки, является недостаточной для обеспечения ПУГЗ ОО.

Проверено, что в документации представлено описание ПУГЗ. Представленное описание является неполным, поэтому процесс оценивания прекращается.

Вариант 6. *Недостаточно = {Не представлено}.*

Документация, в которой описываются процедуры безопасной установки, генерации и запуска объекта оценки не представлена, поэтому процесс оценивания прекращается.

К положительным относятся вердикты со значениями ЛП *достаточно* и *вполне достаточно*, а к отрицательным – *недостаточно*. Уход от бинарной системы принятия решения (т.е. введение промежуточных значений) обусловлено возможностью накопления недостатков. Так, если для уровня гарантии 1 значение ЛП *вполне достаточно* будет допустимым для принятия положительного решения, то на уровне гарантии 2 недостатки первого уровня могут значительно на принятие решения и оказаться критическими. Увеличение количества промежуточных значений приводит к усложнению и разветвлению диаграмм потоков работ в нотации IDEF3, но при наличии инструментальных систем проведения оценивания разумное увеличение количества промежуточных значений повышает точность результатов оценивания.

ЗАКЛЮЧЕНИЕ

Обеспечение требований гарантий безопасности является необходимым условием реализации функциональных требований защищенности и обеспечения безопасности информации в целом. На сегодняшний день в нормативных документах определены подходы и рекомендации относительно выбора требований гарантий и обоснования уровня гарантий для объекта оценки. Однако остаются нерешенными как в теоретическом, так и в практическом плане задачи реализации и оценки выполнения требований гарантий. Учитывая, что требования гарантий носят больше неформальный характер, объектом их приложения являются большей частью организационные и технологические процессы (проектирования, разработки, производства) и для оценки уровня гарантий необходимо использовать различные методы системного анализа.

В статье, на основе анализа предметной области гарантий, устранена неоднозначность в переводе и трактовке англоязычного термина "*assurance*". Авторы стоят на позиции, что термин "*гарантии"* является более подходящим, по сравнению с термином "*доверие"*.

Предлагаемый в данной работе подход позволяет обеспечить требования глубины и строгости оценивания за счет применения методов декомпозиции объектов оценивания свойств гарантий, функционального моделирования процессов оценки и принятия решений о степени проявления свойств гарантий на основе использования лингвистических переменных. В контексте данного подхода проводится анализ объекта оценки и его декомпозиция на свидетельства. Свидетельства используются для оценки множества свойств ОО. Для каждого свойства вводятся ЛП. Формально процесс и порядок оценивания представляется в виде IDEF0 и IDEF3 моделей. Моделирование позволило оптимизировать процесс проведения оценивания и сократить затраты времени и ресурсов на его проведение.

Применение предложенного подхода может послужить основой для проектирования современных инструментальных средств и систем проведения оценивания гарантий безопасности. Подход направлен на создание научно-методического аппарата оценивания гарантий. Его применение не ограничивается использованием только по действующим стандартам [2, 5], а наоборот направлено на облегчение внедрения новых пересмотренных требований гарантий [18, 19] и создание на их основе программ и методик проведения оценивания.

Дальнейшие исследования могут быть направлены на расширение подхода и его более глубокой формализации, а также на поиск методов и способов оценивания отдельных свойств.

Литература.

[1] ISO/IEC 15408-1:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

[2] ISO/IEC 15408-3:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirement.

[3] 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.

[4] НД ТЗІ 2.7-010-09: Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 24.07.2009 №172.

[5] ISO/IEC 18045:2005, Informational technology – Security techniques – Methodology for IT security evaluation.

[6] *Трубачев А.П.* Оценка безопасности информационных технологий / А.П. Трубачев и др. – М.: Издательство СИП РИА, 2001. – 356 с.

[7] ISO/IEC 15443. Informational technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework.

[8] ISO 7498-2:1989. Information processing systems – Open System Interconnection – Basic reference model – Part 2:Security architecture.

[9] NIST SP 800-30. G. Stoneburner. Underlying Technical Models for Information Technology security/- NIST, 2002.

[10] НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

[11] *Грайворонський М.В.* Безпека інформаційно-комунікаційних систем / М.В. Грайводонський, О.М. Новіков – К.: Видавнича група BHV, 2009. – 608 с.

[12] *Палагин А.В., Петренко Н.Г.* Системно-онтологический анализ предметной области. УДК 004.318.

[13] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model. Version 3.1. Revision 3. Final. CCMB-2009-07-001. July 2009.

[14] *Заде Л.А.* Понятие лингвистической переменной и его применение к принятию приближенных решений / Л.А. Заде. – М: Мир, 1976. – 165 с.

[15] *Борисов А.Н.* Модели принятия решений на основе лингвистической переменной / А. Н. Борисов, А. В. Алексеев, О. А. Крумберг и др. – Рига: Зинатне, 1982. – 256 с.

[16] *Саати Т.* Принятие решений. Метод анализа иерархий / Т. Саати. – М.: Радио и связь, 1993. – 278 с.

[17] IDEF5 Method Report. – Armstrong Labarastory AL/HRGA. Wright-Patterson Air Force Base. – 1994.

[18] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components. Version 3.1. Revision 3. Final. CCMB-2009-07-003. July 2009.

[19] Common Methodology for Information Technology Security Evaluation – Evaluation methodology. Version 3.1. Revision 3. Final. CCMB-2009-07-004. July 2009.

Поступила в редколлегию 1.06.2010.

Потий Александр Владимирович, доктор техн. наук, доцент, начальник кафедры радиоэлектронных систем пунктов управления воздушных сил Харьковского университета воздушных сил им. И. Кожедуба. Научные интересы: проектирование комплексных систем защиты информации, криптографических средств защиты информации; методы системного анализа процессов защиты информации; методы оценки безопасности объектов информационной деятельности.

Комин Дмитрий Сергеевич, адъюнкт Харьковского университета воздушных сил им. И. Кожедуба. Научные интересы: методы системного анализа процессов защиты информации; методы оценки безопасности объектов информационной деятельности.

УДК 629.735

Оцінювання гарантій інформаційної безпеки на основі функціонально-лінгвістичного підходу / О.В. Потій, Д.С. Комін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 421-434.

Наводяться результати онтологічного аналізу предметної області оцінювання гарантій інформаційної безпеки. Пропонується підхід до оцінювання рівня гарантій інформаційної безпеки, що базується на функціональному моделювання процесу оцінювання та введенні лінгвістичних змінних, який направлений на виконання вимог глибини та строгості, що висуваються до процесу оцінювання, та вимог об'єктивності, повторюваності, відтворюваності, безпристрасності та співставленості, що висуваються до результатів оцінювання.

Ключові слова: гарантії, рівень безпеки, онтологічне моделювання, оцінювання.

Іл. 10. Бібліогр.: 19 назв.

UDK 629.735

Evaluating assurances of information security on the base of functional-linguistic approach / A.V. Potii, D.S. Komin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 421-434.

The results of the ontological analysis of the subject of evaluating information security assurances are presented. An approach to estimating the level of information security assurances is suggested, which is based on the functional modeling of estimation process and introduction of linguistic variables. The approach is directed on the realization of requirements of depth and rigour to the evaluation process, and requirements of objectivity, repeatability, reproducibility, impartiality and comparability made on evaluation results.

Key words: assurances, security level, ontological modeling, evaluation.

Fig. 10. Ref.: 19 items.

УДК 681.3.06

АНАЛІЗ СИСТЕМ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ

О.В. ПОТІЙ, Д.Ю. ПИЛИПЕНКО

В роботі проаналізовано існуючі на сьогоднішній день системи показників безпеки інформації. Дані системи або таксономії розглянуто як інструмент, здатний надати можливість комплексно охарактеризувати стан безпеки інформації підприємства. Розглядаючи таксономії показників безпеки інформації у такому контексті, були визначені їхні головні властивості, переваги та недоліки.

Ключові слова: показник безпеки інформації, програма забезпечення безпеки інформації, таксономія показників.

ВСТУП

Сьогодні можна із впевненістю говорити, що у галузі інформаційної безпеки (ІБ) особа, що приймає рішення (ЛПР) вже не може спиратися лише на інтуїцію. Прийняттю більш обґрунтованих рішень можуть сприяти показники безпеки, користуючись якими ЛПР отримає можливість приймати рішення, вважаючи умови динамічного мінливого середовища.

На прийняття рішень впливають фактори: суб'єктивні (досвід ЛПР, що є результатом прийнятих у минулому рішень та отриманих наслідків, знання ЛПР у цій галузі, інтуїція) та об'єктивних (різного роду показники). Перша група факторів в значній мірі залежать від особистості ЛПР, і вплинути на них важко. Проте, за допомогою об'єктивних показників безпеки інформації можна сформувати інформаційну повноту, спираючись на яку ЛПР зможе прийняти більш обґрунтоване рішення.

У 2001 р. пройшла перша конференція, що була повністю присвячена питанням оцінювання інформаційної безпеки, – Workshop on Information, Security System Scoring and Rankin. В матеріалах даної конференції [1] містяться ключові погляди фахівців у галузі інформаційної безпеки, обговорюється безліч проблем, пов'язаних з оцінюванням інформаційної безпеки. З цього моменту в англомовній літературі починає активно вживатись термін «security metrics», який на українську мову можна перекласти як метрика безпеки або – більш коректно – показник безпеки. Необхідно зауважити, що через різні переклади використовуються різні поняття, і тлумачення самих понять також не завжди співпадає. Це призводить до певної плутанини у термінах, тому на даний момент існує потреба в єдиній затвердженій терміносистеми у напрямку оцінювання безпеки інформації.

1. ТАКСОНОМІЯ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ VAUGH–HENNIG–SIRAJ

В роботі [2] підбиваються підсумки конференції WISSRR [1] та обговорюються ключові проблеми, що з'явилися під час проведення досліджень у цьому напрямку. Автори запропонували та обґрунтували свою версію таксономії показників безпеки. Ефективність набору показників безпеки з точки зору авторів залежить від цілої низки факторів: поставлених задач безпеки; технічних, організаційних та операційних потреб; доступних фінансових, кадрових та технічних ресурсів.

Під час створення цієї системи показників безпеки автори в деякій мірі користувалися спостереженнями Дебори Бодо [2], якою було запропоновано розглядати показники як векторний добуток об'єкта вимірювань, мети вимірювань та особи, для якої призначені результати вимірювань. Рис 1. ілюструє цю концепцію:

Різноманіття підприємств, діяльність яких відбувається у своєму специфічному середовищі, дійсно створює ситуацію, коли одним набором показників неможливо задовольнити усі потреби. На вибір показників безпеки інформації неминуче впливає розмір підприємства, доступні ресурси та рівень зрілості процесів підприємства.

Інформаційна безпека з точки зору авторів становить поєднання трьох елементів, а саме *тех-*

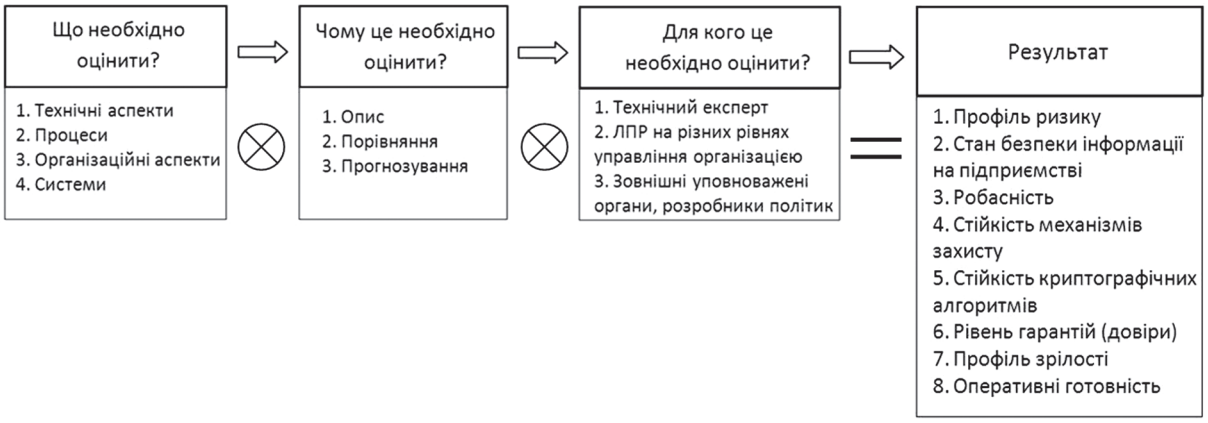


Рис. 1. Модель показника безпеки інформації Бодо

нології, що обумовлює захист, *процесу*, в котрому ця технологія використовується, та *людей*, завдяки яким ця технологія працює. Розвиваючи цю ідею, можна припустити, що показники безпеки інформації повинні охоплювати усі три елемента – продукт, процес та кадри.

Було запропоновано поділити усі показники безпеки на дві категорії: *організаційні показники безпеки* та *показники оцінювання технічних об'єктів* (рис. 2). Організаційні показники використовуються для оцінювання ефективності/результативності програми забезпечення безпеки інформації (програма ЗБІ) та процесів захисту інформації, впроваджених на підприємстві. За допомогою цих показників формується зворотній зв'язок у циклі управління та вдосконалення діяльності з забезпечення безпеки інформації. Клас показників оцінки технічних об'єктів впроваджено для оцінювання того, наскільки добре технічні об'єкти (продукти, системи, засоби захисту тощо) здатні забезпечити довіру (гарантії) у термінах захисту від атак, їх виявлення та реагування на інциденти безпеки.

Ключовою особливістю даної роботи є вперше запропонована цілісна таксономія показників безпеки інформації. Ця таксономія поєднує різні групи показників та дозволяє охарактеризувати діяльність підприємства у контексті забезпечення безпеки інформації. Проте, авторами не було запропоновано конкретних показників. Рішення цієї задачі було покладено безпосередньо на фахівців, що будуть адаптувати запропоновану таксономію до конкретних специфічних умов свого підприємства.

2. ТАКСОНОМІЯ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ OCTAVE

У 2001-2003 роках інститутом SEI було розроблено метод OCTAVE (Operational Critical Threat, Asset and Vulnerability Evaluation), що дозволяє підприємству ідентифікувати ризики для своїх найбільш важливих інформаційних активів та розробити стратегічній план усунення виявлених ризиків безпеки [3]. В рамках цього методу виділяється етап оцінювання поточного стану діяльності з захисту інформації. Для рішення цієї задачі було розроблено каталог практик безпеки та спеціальну анкету, які, по суті, являють собою засіб оцінювання поточної практики безпеки на підприємстві та формування відповідної стратегії покращення практичної діяльності для забезпечення більш ефективного захисту критичних активів. На рис. 3 наведено таксономію показників безпеки інформації, розроблену згідно з каталогом практик безпеки OCTAVE [3]. Декомпозиція показників обґрунтовується тим, що метод OCTAVE, насамперед, орієнтовано на рішення проблем безпеки, пов'язаних не з технологіями, а з практичною діяльністю. Цей метод працює у площині операційних ризиків безпеки та практики безпеки інформації, а технологія розглядається тільки по відношенню до практики безпеки. Розробники каталогу практик безпеки спиралися на декілька джерел, головним чином на нормативні документи [4, 5], а також на власні розробки інституту SEI.

Отже, всю множину показників безпеки було поділено на два класи: показники стратегічної та операційної діяльності із забезпечення безпеки інформації. Вони складають перший рівень ієрархії.

Показники стратегічної діяльності, насамперед, орієнтовані на оцінювання організаційних проблем на рівні політик безпеки інформації та корпоративного управління безпекою. Стратегічна діяльність пов'язана із загальними бізнесцілями підприємства та потребує наявності корпоративних планів та участі вищого керівництва у вирішенні цих проблем. Показники операційної діяльності використовуються для оцінювання проблем, пов'язаних здебільшого з використанням технологій захисту у повсякденній діяльності співробітників підприємства.

Рис. 2. Таксономія показників безпеки інформації Vaugh–Hennig–Siraj

На другому рівні ієрархії вводяться підкласи стратегічних показників (6 підкласів) та операційних показників (3 підкласи), які в свою чергу також розкладаються на підкласи. У кожному підкласі другого рівня стратегічних показників і третього рівня операційних показників визначаються декілька чинників, що підлягають оцінюванню. Наприклад, у класі стратегічних показників оцінювання стратегії захисту виділяються показники, що характеризують:

• облік бізнес-стратегій під час розглядання питань з безпеки інформації;

• облік стратегії безпеки у загальних стратегічних цілях та задачах підприємства;

• якість та періодичність перегляду та оновлення документації, від ображаючої стратегію безпеки, цілі та задачі захисту.

У класі операційних показників криптографічного захисту вводяться показники, що характеризують:

• застосування засобів криптографічного захисту інформаційних активів;

• застосування криптографічних протоколів під час передачі інформації, реалізації віддаленого доступу до ресурсів;

• періодичність аналізу, верифікації та модифікації криптографічних засобів захисту інформації та протоколів.

Оцінювання є якісним та здійснюється методом експертного опиту та аналізу стану практики інформаційної безпеки на підприємстві. Таксономія OCTAVE складається з показників якісного типу. Наведена методика не надає чітких інструкцій відповідно того, яким чином необхідно організовувати процес моніторингу ризиків.

3. ТАКСОНОМІЯ ПОКАЗНИКІВ БЕЗПЕКИ ОСІРЕР

Цю таксономію було розроблено у 2004 р. групою канадських фахівців для уряду Канади (Департамент захисту критичної інфраструктури та надзвичайних ситуацій) [6]. Під час розробки цієї таксономії автори дотримувалися ширших поглядів щодо оцінювання безпеки інформації. Вони висловлюють наступну ідею: оцінювання безпеки інформації повинно формуватися у рамках *концепції інформаційної довіри* чи *інформаційних гарантій* (Information Assurance, IA), або *гарантій інформаційної інфраструктури* (Information Infrastructure Assurance). Під цим терміном автори розуміють здатність мереж та систем забезпечити своєчасну передачу інформації між двома або більше сторонами із заданою точністю та безпекою. Інформаційна довіра складається з трьох базових елементів: забезпечення безпеки інформації (Security Information), забезпечення якості послуг (Quality of Service, QoS) та доступність IT-інфраструктури (Availability). Спираючись на приведене визначення IA та три ключових елементи інформаційної довіри, автори пропонують свій варіант таксономії. При цьому основним об'єктом оцінювання стають системи інформаційних технологій та мереж.

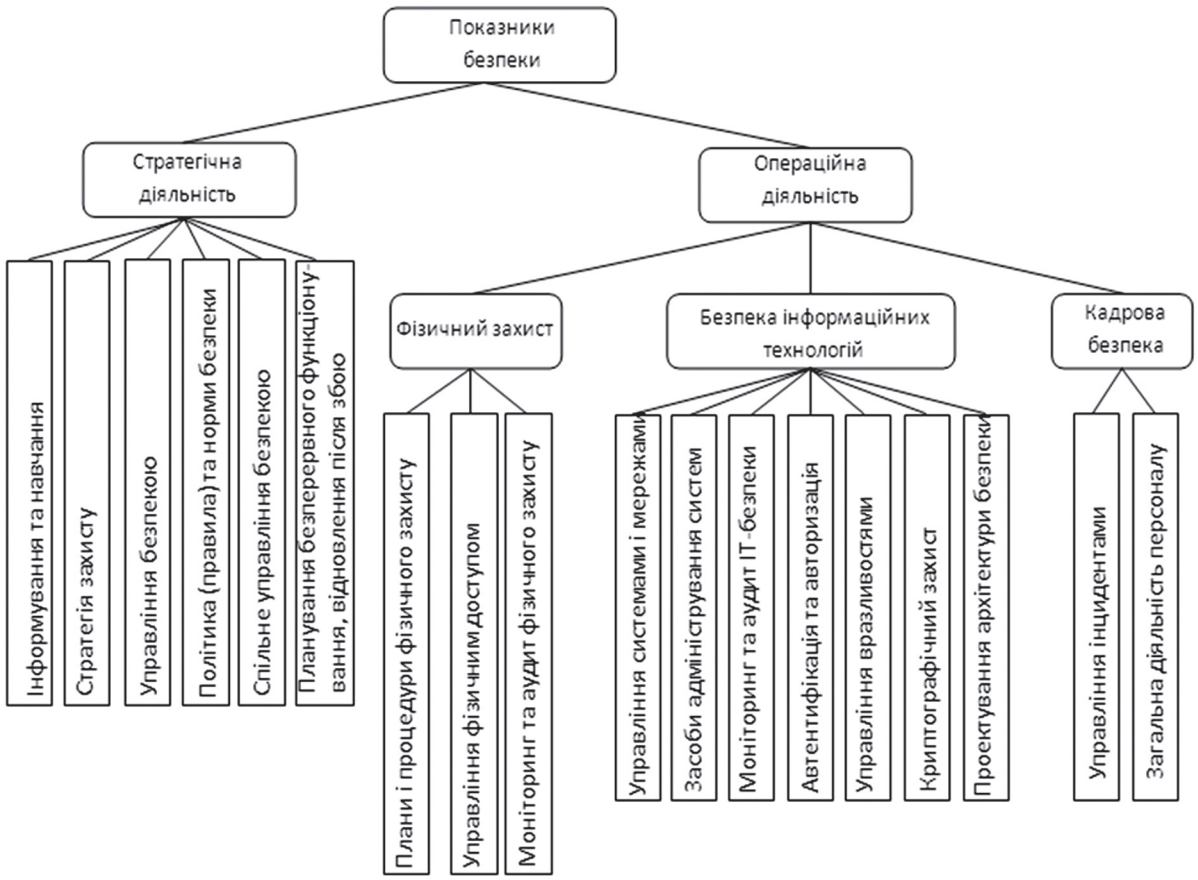


Рис. 3. Таксономія показників безпеки інформації OCTAVE

Таксономія показників OCIPEP є багаторівневою (рис. 4). Перший рівень ієрархії формується по ключовим елементам ІА. Другий рівень ієрархії формується таким само чином, як і в таксономіях WISSRR, Vaugh–Hennig–Siraj та NIST, тобто вся множина показників поділяється на показники організаційного управління, показники оцінювання операційної практики захисту інформації та показники оцінювання технічних елементів.

Далі відбувається більш детальна декомпозиція показників у кожному класі. Група показників організаційного управління використовується для оцінювання того, яка увага приділяється питанням забезпечення безпеки інформації. До цієї групи належать показники, що характеризують такі аспекти, як розробка програми ЗБІ (оцінювання якості планування захисту, управління ризиками безпеки, розробка політики безпеки) та управління ресурсами (кадрове забезпечення та матеріально-технічне забезпечення захисту інформації).

Група операційних показників характеризує підприємство з точки зору досягнення цілей безпеки, виконання політики безпеки та вирішування задач захисту. Ця група складається з показників технічної готовності (якість документування, цілісність даних, якість планування безперервного функціонування), оцінювання вразливостей мережі у конкретному середовищі безпеки, ефективність діяльності із захисту інформації.

Група показників оцінювання технічних елементів використовується для оцінювання того, наскільки вимоги безпеки інформації забезпечуються технічними компонентами мережі. До цієї групи належать статистичні показники оцінювання засобів захисту інформації (програмних, апаратних, програмно-апаратних засобів), статистичні показники інцидент інцидентів безпеки у мережі (системі), динамічні показники тестування безпеки (тестування на проникання, тестування на відмову в обслуговуванні).

Під час розробки таксономії показників OCIPEP автори спирались на таксономії NIST, WISSSR та Vaughn–Hennig–Siraj, розглядаючи можливість сформувати з них фундамент для таксономії, яку можна використовувати для оцінювання комп'ютерних мереж. Автори дійшли наступних висновків: наведені таксономії не можуть бути застосовані для оцінювання стану комп'ютерної мережі по трьом факторам, а саме захищеності, доступності та QoS. Таким чином, авторами було запропоновано нову таксономію та категорію показників, за допомогою яких можна отримати оцінювання інформаційних гарантій для комп'ютерної мережі. Слід зауважити, що в рамках таксономії OCIPEP не було запропоновано конкретних показників та методології проведення вимірювань.

4. ТАКСОНОМІЯ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ CISWG

В 2004 році робочою групою корпоративної інформаційної безпеки (Corporate Information Security Working Group, CISWG) підкомітету технологій, інформаційної політики та міжурядових взаємодій уряду США було підготовлено звіт, що містив рекомендації щодо найкращих практик безпеки (діяльність із захисту інформації). Наведені рекомендації інтерпретувались як складові елементи програми ЗБІ, а також у якості підтримки до них було запропоновано кількісні показники безпеки інформації [7]. Запропонована система практик може бути використана будь-якими підприємствами (державними, академічними, комерційними) для розробки програми ЗБІ або удосконалення вже існуючої. Автори підкреслюють, що основною їхньою задачею була розробка ресурсу, користуючись яким, керівництво, менеджери та технічний персонал отримає можливість розробити свій комплекс принципів, політик, процесів, засобів захисту та показників продуктивності, спрямованих на співробітників, процеси та технологічні аспекти інформаційної безпеки.

Автори акцентують увагу на тому, що відправним пунктом в формуванні програми ЗБІ є запропонований керівництвом набір принципів, на базі якого і буде сформовано комплекс заходів, що складається з політики безпеки, процесів, заходів із забезпечення безпеки інформації та показників продуктивності. Даний момент вартий уваги з приводу того, що автори пропонують спадний підхід до формування програми ЗБІ. Ідея включення у цей процес також і вищого керівництва, безперечно, корисна, оскільки подібна взаємодія керівництва та співробітників, що безпосередньо зайняті організацією безпеки інформації, сприятиме узгодженню бізнес-цілей підприємства та цілей ІБ.

Запропонована таксономія показників дозволяє будь-якому підприємству розробити свою систему показників для оцінки ефективності ре-

Рис. 4. Загальна таксономія показників безпеки інформації OCIPEP

алізації програми ЗБІ. Показники демонструють те, наскільки ефективно здійснюються політики безпеки, процеси та заходи захисту інформації, чи досягаються поставлені цілі безпеки. Наведені у цій роботі показники вимірюють стан або ефективність реалізації заходів захисту інформації, проте не стосуються пов'язаних з цим ризиків. Управління ризиками потребує додаткових робіт, які складаються з виявлення ймовірності реалізації загроз, виявлення вразливостей та можливих збитків.

Показники безпеки дозволяють здійснювати безперервне покращення процесів, сприяють зростанню рівня зрілості процесів, оскільки вони надають об'єктивний спосіб оцінювання стану певного об'єкту інформаційної безпеки. На рис. 5 наведена таксономія показників безпеки, розроблена на базі елементів загальної програми ЗБІ CISWG.

Таксономія CISWG налічує 99 показників безпеки інформації. Уся множина показників поділена на три групи: показники підтримки стратегічної практики управління безпекою (7 напрямків діяльності та 12 показників), показники підтримки оперативного управління (10 напрямків та 42 показники безпеки) та показники підтримки технічної діяльності із захисту інформації (13 напрямків та 45 показників безпеки інформації). Робоча група виокремлює 65 базових показників, тобто мінімально необхідну множину показників, які дозволяють проводити оцінювання тринадцяти базових практик безпеки. Ці базові практики є початковою точкою в процесі реалізації програми ЗБІ. Для підприємств чисельністю менш ніж 500 осіб (малі та середні підприємства) визначено п'ять фундаментальних практик безпеки, які спираються на множину із 40 показників безпеки інформації.

Відмітною особливістю наведеної таксономії показників безпеки інформації є те, що усі показники кількісні та представлені у вигляді процентів. Під час розробки системи практик робоча група спиралась на розробки NIST [8] та систему оцінювання корпоративної інформаційної безпеки ISG.

Рис. 5. Таксономія показників безпеки інформації CISWG

5. ТАКСОНОМИЯ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ ERKAN KAHRAMAN

Таксономія показників безпеки Erkan Kahraman (Стокгольмський університет) становить собою академічну розробку, запропоновану та створену автором у 2004 році [9]. Автор поставив перед собою мету розробити зручний інструмент, здатний підвищити ефективність управління безпекою, виконання аналізу ризиків, прийняття стратегічних рішень у контексті забезпечення безпеки інформації. Головним принципом, який було покладено автором в основу таксономії, є необхідність показників піддаватись кількісному обчисленню (наприклад, проценти, абсолютне число, відносне число). Показники також повинні легко визначатися та відзначатися певною гнучкістю під час вимірювань. Автор поставив перед собою наступні питання:

• Чи можливе вимірювання інформаційної безпеки підприємства взагалі?

• Якому рівню інформаційної безпеки відповідають певні значення показників безпеки?

• Як змінюється рівень інформаційної безпеки підприємства з часом?

Особливу увагу автор приділяє питанням оцінювання виконання тієї чи іншої діяльності із захисту інформації (security performance), оцінювання результативності та ефективності процесу забезпечення безпеки інформації. Формулювання цілей та задач безпеки інформації на думку автора необхідно здійснювати у формі високорівневих вимог політик безпеки. Автор вводить Ключові Індикатори Виконання (Key Performance Indicators, KPI), до яких відносяться:

• ефективність та результативність політик безпеки;

• вплив рівня компетентності на дії співробітників;

• робасність мереж та систем;

• реагування на інциденти безпеки та безперервне функціонування;

• управління доступом.

Показники безпеки пропонується визначати на основі трьох методів: методом контрольного списку (експертна оцінка по шкалі «так» (0) або «ні» (1)); методом бальної експертної оцінки у довільних шкалах та методом розрахунку показника шляхом об'єктивних вимірювань (у вигляді процентів). Процедура оцінювання здійснюється шляхом відповіді на поставлені питання. Всього сформульовано 90 питань.

6. ТАКСОНОМИЯ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ NIST

У 2005 році було завершено роботу рекомендацій NIST SP 800-53A [10]. Цей нормативний документ закріплює таксономію показників безпеки, побудовану на базі класифікації заходів захисту NIST SP 800-53 [11] (рис. 7).

У цілому таксономія NIST складається з трьох груп показників безпеки, що у свою чергу об'єднують 17 класів показників, які характеризують різні сімейства заходів захисту інформації (на рис. 9. наведено назви сімейств та їхні ідентифікатори). Слід зазначити, що запропонована класифікація помітно корелює із такими міжнародними стандартами, як ISO/IEC 17799 [4], ISO/IEC 13335 [12], а також з іншими нормативними документами США у сфері інформаційної безпеки. Це дозволяє зробити наступний висновок: підходи, застосовані під час розробки таксономії NIST досить легко адаптувати та розповсюдити на вимоги міжнародних стандартів, і таким чином побудувати відповідні таксономії показників безпеки.

Окрім того, в таксономії показників безпеки NIST досить чітко визначено об'єкт оцінювання

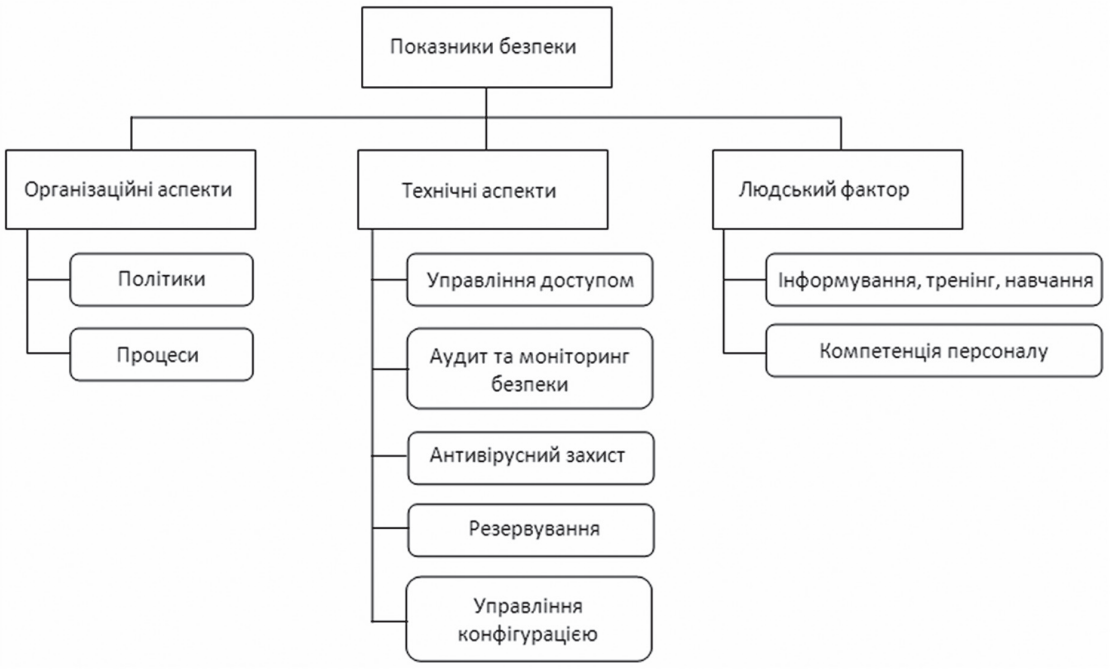


Рис. 6. Таксономія показників безпеки інформації Erkan Kahraman

– це заходи захисту, що реалізуються в інформаційних системах урядових закладах США. Використанню наведеної системи показників безпеки в урядових закладах приділяється велике практичне значення.

Зазначимо, що усі класи показників безпеки пропонується використовувати на організаційному рівні. Інакше кажучи, група технічних показників має мету оцінити рівень технічних засобів захисту інформації, що використовується на підприємстві. На відміну від таксономії Vaugh–Hennig–Siraj, група технічних показників NIST не призначена для оцінювання конкретного технічного об'єкту. Зазначимо також, що під час розробки таксономії NIST не було визначено критерії, у відповідності до яких здійснюється розбиття загальної множини показників на групи операційних, технічних або організаційних показників.

В рекомендаціях NIST SP 800-55 [8] у залежності від рівня виконання Програми ЗБІ, вводяться три типи показників безпеки:

• показники реалізації (виконання) заходів захисту інформації;

• показники результативності заходів;

• показники оцінки впливу заходів захисту на цільову функцію підприємства.

Показники різних типів можна використовувати одночасно. Проте, у залежності від рівня виконання програми ЗБІ виділяється і основний тип показників, що використовуються.

Якщо програма ЗБІ представлена у вигляді процедур (або процесів) і виконується у фокусі оцінювання реалізації елементів програми, тоді основними будуть показники виконання (наприклад, доля систем із затвердженими планами захисту). На першому та другому рівні виконання програми ЗБІ значення показників буде знаходитись у межах від 0 до 100%. На третьому рівні виконання програми припускається, що ці показники досягнуть максимального 100%-го рівня. Коли діяльність із захисту інформації стає систематичною, цілеспрямованою, керованою, а дані відносно її реалізації більш доступними та об'єктивними, основними показниками безпеки стають показники оцінювання результативності (наприклад, оперативність реагування на інциденти безпеки, своєчасність надавання послуг безпеки). Фокус уваги ЛПР зміщується з вирішень задач реалізації у бік вирішення задач забезпечення ефективності програми ЗБІ.

Показники впливу стають основними у разі повної інтеграції діяльності із захисту інформації у бізнес-процеси підприємства. Такі показники визначають, наприклад, кількість інцидентів безпеки за типами та їхню кореляцію з рівнем підготовки персоналу, або кількість втрачених клієнтів компанії через зниження репутації. Таким чином, на 4 та 5 рівнях виконання програми ЗБІ особливої ваги набувають показники ефективності і оцінювання корисності захисту інформації для підприємства.

7. ГОЛОВНІ ПРОБЛЕМИ РОЗРОБКИ ТА ІНТЕГРАЦІЇ ПОКАЗНИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні існують певні фактори, що перешкоджають широкому використанню та інтеграції показників безпеки:

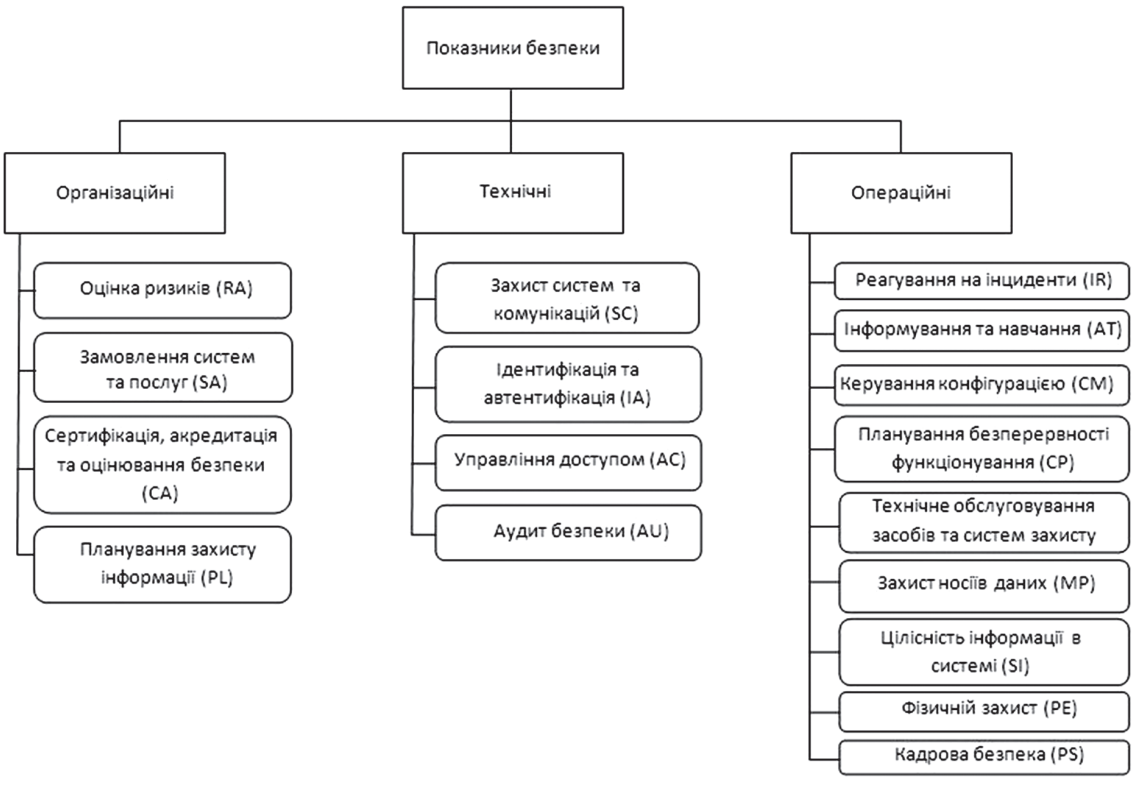


Рис. 7. Таксономія показників безпеки інформації NIST

• Неясність терміну «показник безпеки», "security metric", недостатня об'єктивність результатів процесу оцінювання;

• Певні труднощі в отриманні кількісних результатів оцінювання об'єктів інформаційної безпеки;

• Труднощі з оцінювання операційних показників безпеки;

• Сам по собі характер проблем інформаційної безпеки.

Оцінювання людського фактора в контексті інформаційної безпеки є важливою задачею, проте нетривіальною. Існує протиріччя між оцінюванням безпеки та захистом особистої інформації, тому досить зрозумілим є бажання не завдати шкоди особистим інтересам людини, діяльність якої буде підлягати оцінюванню. З цієї позиції важливими напрямками є оцінювання вмотивованості, лояльності, компетенції, знань та досвіду співробітників у сфері інформаційної безпеки. Виділимо основні проблеми, що стосуються різних аспектів безпеки інформації.

Проблеми та задачі в області поведінкового аспекту:

• Щоденне оцінювання діяльності із забезпечення безпеки інформації;

• Оцінювання рівня культури інформаційної безпеки на підприємстві;

• Оцінювання поведінки співробітників;

• Оцінювання процесів навчання співробітників у сфері інформаційної безпеки.

Проблеми розробки організаційних та операційних показників безпеки інформації:

• Якісне оцінювання рівня безпеки інформації;

• Внутрішній аудит;

• Досягнення оптимального рівня безпеки систем;

• Необхідність введення базового рівня безпеки інформації;

• Зручність використання показників безпеки;

• Автоматизація збору даних;

• Мінімізація кількості показників безпеки інформації;

• Інтеграція показників безпеки у бізнес-процеси підприємства.

Складності технічного характеру:

• Ведення та аналіз журналів контролю;

• Необхідність аналізу мереж;

• Технічні засоби, що дозволяють автоматизацію;

• Відстеження вірусів та їх локалізація в системах та мережах;

• Безумовна стійкість продуктів, процесів та робіт;

• Самонавчання.

ВИСНОВКИ

Проаналізувавши існуючі на сьогоднішній день таксономії показників безпеки інформації, можна дійти висновку, що взагалі існує три типи систем: таксономії, що містять виключно кількісні показники (CISWG); таксономії, що містять виключно якісні показники (OCTAVE); таксономії змішаного типу, що містять показники обох типів (NIST, Erkan Kahraman). Таким чином, усі існуючі на сьогоднішній день таксономії спираються на розділення усієї множини показників на три категорії: організаційні, операційні та технічні показники. Це говорить про те, що серед фахівців склався погляд, що усебічне оцінювання рівня безпеки інформації можна провести тільки враховуючи різних факторів та аспектів захисту інформації. Головний та спільний для цих таксономій недолік – це відсутність рекомендацій щодо розробки комплексних, інтегральних показників. Це є досить суттєвим недоліком, оскільки вище керівництво зацікавлене у інтегральних показниках безпеки в контексті прийняття стратегічних рішень.

Інша значна проблема стосується інтерпретації конкретних значень показників безпеки (які в свою чергу можуть бути представлені у різних формах). Наприклад, керівнику служби безпеки доповідають «коефіцієнт персоналу, що пройшов тренінг з безпеки, становить 0.62». Одразу ж виникає питання, достатньо цього значення чи ні. Таким чином, саме лінгвістична оцінка впливає на ЛПР як значущий сигнал та найкращим чином спонукає його до прийняття рішення.

Запропоновані фахівцями таксономії здебільшого вирішують проблему формування множини показників, що дозволять провести усебічне оцінювання стану безпеки інформації на підприємстві. Проте, в існуючій літературі відсутні будь-які методи або засоби узагальнення показників, тим самим отримуючи інтегральні оцінки стану безпеки інформації.

Література.

[1] Workshop on Information, Security System Scoring and Ranking (WISSSR, 2001) Information System Security Attribute Quantification or Ordering (Commonly but improperly known as Security Metrics) – Workshop Proceedings – May 21-23, 2001, Williamsburg, VA.

[2] *Rayford Vaughn Jr., Ronda Henning, Ambareen Siraj,* Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, 30th Hawaii International Conference on System Sciences, Big Island, Hawaii, January 7- 10, 2002.

[3] *Alberts C., Dorofee A.* Managing Information Security Risks "The OCTAVE Approach" Addison-Wesley Publishing 2003.

[4] NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996

[5] ISO/IEC 17799:2005 (BS 7799-1:2005) Information technology. Security techniques. Code of practice for information security management.

[6] *Seddigh N, P Pieda, A Matrawy, B Nandy, J Lambadaris, and A Hatfield.* 2004. "Current Trends and Advances in Information Assurance Metrics." Proceedings of the

Second Annual Conference on Privacy, Security and Trust (October 2004).

[7] Corporate Information Security Working Group (CISWG). November 17, 2004 (Revised January 10, 2005). Report of the Best Practices and Metrics Teams, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Government Reform Committee, United States House of Representatives.

[8] NIST SP 800-55, Security Metrics Guide for Information Technology Systems, July 2008.

[9] *Erkan Kahraman*. Evaluating it security performance with quantifiable metrics. Master's thesis, DSV SU/KTH, 2005.

[10] NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 2008.

[11] NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Aug. 2009.

[12] ISO/IEC 13335-1:2004 Information technology. Security techniques. Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management.

Надійшла до редколегії 7.06.2010.

Потій Олександр Володимирович, доктор техн. наук, доцент, начальник кафедри радіоелектронних систем пунктів управління повітряних сил Харківського університету повітряних сил ім. І. Кожедуба. Область наукових інтересів: проектування комплексних систем захисту інформації, криптографічних засобів захисту інформації; методи системного анализу процесів захисту інформації; методи оцінки безпеки об'єктів інформаційної діяльності.

Пилипенко Дмитрий Юрьевич, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: комплексные системы защиты информации, управление информационной безопасностью.

УДК 681.3.06

Анализ систем показателей безопасности информации / А.В. Потий, Д.Ю. Пилипенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 435-443.

В работе проведен анализ существующих на сегодняшний день систем показателей безопасности информации. Данные системы или таксономии были рассмотрены в качестве инструмента, способного предоставить возможность комплексно охарактеризовать состояние безопасности информации на предприятии. Рассматривая показатели безопасности в данном контексте, были выделены их ключевые особенности, преимущества и недостатки.

Ключевые слова: показатель безопасности информации, программа обеспечения безопасности информации, таксономия показателей безопасности.

Ил. 07. Библиогр.: 12 назв.

UDC 681.3.06

Analysis of security metrics taxonomies / A.V. Potii, D.Yu. Pilipenko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 435-443.

The paper presents analysis of existing security metrics taxonomies. The security metrics taxonomies have been considered as an instrument, which allows comprehensive information security assessment within an organization. Analyzing the security metrics taxonomies in terms of information security evaluation, the most significant features, advantages and disadvantages have been defined.

Key words: security metrics, security program, security metrics taxonomy.

Fig. 07. Ref.: 12 items.

УДК 321.2

СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ МЕТОДОВ ИДЕНТИФИКАЦИИ ТРАФИКА В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ДЛЯ ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ ПЕРЕДАЧИ ДАННЫХ

С.Г.СЕМЕНОВ, Е.В.МЕЛЕШКО

Определены перспективные направления повышения оперативности передачи данных. Проведены сравнительные исследования методов идентификации трафика в телекоммуникационной сети. Представлены математические модели систем параметрической и структурной идентификации. Выявлены достоинства и недостатки различных методов идентификации, а так же возможности по использованию этих методов для идентификации трафика в телекоммуникационной сети. Предложены пути дальнейших исследований и разработки метода структурной идентификации трафика для повышения оперативности передачи данных.

Ключевые слова: телекоммуникационные сети, идентификация трафика, оперативность передачи данных.

ПОСТАНОВКА ПРОБЛЕМЫ

В соответствии с концепцией государственной информационной политики Украины одним из приоритетных направлений развития единой информационно-телекоммуникационной инфраструктуры является качественное совершенствование системы передачи данных на основе внедрения современных информационных и телекоммуникационных технологий, применение новейших методов и средств цифровой передачи информации.

Анализ государственных стандартов Украины (ДСТУ 2941-94, ГОСТ 34.003-90 и др.), рекомендаций международного союза электросвязи (МСЭ) (МСЭ Е.430, Е.800, Х.134 –137 и др.) показал, что современная система передачи и отображения данных должна обеспечивать качество услуг, связанных с передачей в цифровом виде команд и формализованных сообщений, текстовой и графической информации, аудиосигналов и видеоинформации, а так же данных измерений некоторых физических систем (объектов).

Проведенный анализ информационных и телекоммуникационных технологий [2, 4] показал, что в настоящее время требования к показателям качества передачи данных обеспечиваются с помощью механизмов и средств (протоколов), используемых на разных уровнях модели взаимодействия открытых систем.

Следует отметить, что исторически для обеспечения качества передачи данных на практике чаще использовались механизмы и средства физического и канального уровней. Однако при насыщении рынка телекоммуникаций современными технологиями канального и физического уровней и значительном увеличении интенсивности потока информации в ТКС решение задачи обеспечения требуемых показателей качества передачи данных только лишь на этих уровнях теряют актуальность. В этом случае экономически целесообразно усовершенствовать алгоритмы и процедуры управления ресурсами телекоммуникационных сетей, реализованные на верхних уровнях модели ВОС, и в совокупности с новейшими разработками физического и канального уровней, решать поставленные перед операторами ТКС задачи.

Одним из путей такого усовершенствования является разработка и применение новых методов идентификации трафика в процессе маршрутизации информации.

Целью данной статьи является сравнительное исследование существующих методов идентификации трафика в ТКС.

ОСНОВНАЯ ЧАСТЬ

Проведенные исследования показали, что при решении задач идентификации трафика выделяют методы структурной (непараметрической) и параметрической идентификации.

Анализ ряда работ в области идентификации объектов управления [1-6] показал, что наиболее распространенными методами решения задач параметрической идентификации объектов являются методы наименьших квадратов, вспомогательных переменных, максимального правдоподобия и стохастической аппроксимации.

Как показали исследования, все указанные методы параметрической идентификации могут быть приведены к единой форме описания:

$$\hat{\theta}(k+1) = \hat{\theta}(k) + \gamma(k)e(k+1); \qquad (1)$$

$$\gamma(k) = \mu(k+1)P(k)\varphi(k+1); \qquad (2)$$

$$e(k+1) = y(k+1) - \Psi^T(k+1)\hat{\theta}(k), \qquad (3)$$

где $\hat{\theta}(k)$ – вектор параметров оценки; $e(k)$ – вектор ошибок идентификации; $y(k)$ – выходные данные; $\gamma(k)$ – вектор коррекции ошибок; $\Psi^T(k)$ – вектор выходных данных.

Анализ перечисленных методов параметрической идентификации, а также модели системы идентификации, представленной выражениями 1-3, показал, что отличительными характерис-

тиками для различных методов идентификации являются векторы параметров $\hat{\theta}(k)$, векторы данных $\Psi\ (k+1)$ и векторы коррекции $\gamma(k)$.

Так, например, математическую модель системы параметрической идентификации, основанную на методе наименьших квадратов, можно представить в виде выражений:

$$\hat{\theta}(k-1)=[a_1,....a_n,b_1,.....b_m],$$

$$\Psi^T(k)=$$

$$=[-y(k-1),...-y(k-n),u(k-d-1),...+u(k-d-m)],$$

$$\mu(k+1)=\frac{1}{1+\Psi^T(k+1)P(k)\Psi(k+1)},$$

$$P(k)=\frac{1}{\left[\Psi^T(k)\Psi(k)\right]},$$

$$P(k+1)=\left[I-\gamma(k)\Psi^T(k+1)\right]P(k),$$

$$\varphi(k+1)=\Psi(k+1),$$

$$\hat{\theta}(0)=0;\quad P(0)=\alpha I.$$

Математическую модель системы параметрической идентификации, основанную на рекуррентном методе вспомогательных переменных, можно представить в виде:

$$\hat{\theta}(k-1)=[a_1,....a_n,b_1,.....b_m];$$

$$\Psi^T(k)=$$

$$=[-y(k-1),...-y(k-n),u(k-d-1),...+u(k-d-m)];$$

$$\varphi^T(k)=[-h(k-1),...-h(k-n),u(k-d-1),...u(k-d-n)];$$

$$h(k)=\varphi^T(k)\hat{\theta}_b(k);$$

$$\hat{\theta}_b(k)=(1-\beta)\hat{\theta}_b(k-1)+\beta\hat{\theta}(k-\eta),\quad 0{,}01\le\beta\le 0{,}1;$$

$$\mu(k+1)=\frac{1}{1+\Psi^T(k+1)P(k)\Psi(k+1)};$$

$$P(k+1)=\left[I-\gamma(k)\varphi^T(k+1)\right]P(k);$$

$$\nu(0)=y(0);\quad \hat{\theta}(0);\quad P(0)=\alpha I.$$

Математическую модель системы параметрической идентификации, основанную на методе максимального правдоподобия в виде:

$$\hat{\theta}^T=[\hat{a}_1,....\hat{a}_n,\hat{b}_1,.....\hat{b}_n,\hat{d}_1...\hat{d}_n];$$

$$\varphi^T(k+1)=\left[-\begin{pmatrix}y'(k),...-y'(k-n+1),\\u'(k-d),...u'(k-d-n+1),\\e'(k),...e'(k-n-1)\end{pmatrix}\right];$$

$$y'(k)=y(k)-\hat{d}_1\,y'(k-1)-...-\hat{d}_n\,y'(k-n);$$

$$u'(k)=y(k-d)-\hat{d}_1\,u'(k-d-1)-...-\hat{d}_n\,u'(k-d-n);$$

$$e'(k)=e(k)-\hat{d}_1\,e'(k-1)-...-\hat{d}_n\,e'(k-n);$$

$$\mu(k+1)=\frac{1}{1+\varphi^T(k+1)P(k)\varphi(k+1)};$$

$$P(k+1)=\left(I-\gamma(k)\varphi^T(k+1)\right)P(k);$$

$$\theta(0)=0,\quad P(0)=\alpha I,\quad \varphi(0)=0.$$

Математическую модель системы параметрической идентификации, основанную на методе стохастической аппроксимации в виде:

$$\hat{\theta}(k-1)=[a_1,....a_n,b_1,.....b_m];$$

$$\Psi^T(k)=\begin{bmatrix}-y(k-1),...-y(k-n),\\u(k-d-1),...+u(k-d-m)\end{bmatrix};$$

$$\mu(k+1)=1;$$

$$P(k+1)=\frac{c}{k+1};$$

$$\varphi(k+1)=\Psi(k+1);$$

$$\hat{\theta}(0)=0,\quad P(0)=\alpha I.$$

Если считать, что параметры идентифицируемого объекта на интервале измерений $k=0....N$ оставались постоянными, то изменения $u(k)$, $y(k)$ и ошибки $e(k)$ входят во все отношения с одинаковыми весами, не зависящими от k.

Результаты исследований параметрических методов идентификации [3-6] показали, что основным достоинством указанных методов параметрической идентификации является относительная точность оценки параметров трафика. Однако в условиях влияния на трафик различного рода помех точность такой оценки значительно ухудшается. Кроме этого большой объем вычислений, требуемый для параметрической идентификации, и низкая сходимость оценок динамически изменяемых параметров информационного трафика в настоящее время не позволяют реализовать эти методы на практике. Поэтому многие разработки в области идентификации в настоящее время связаны с непараметрической оценкой информационного трафика.

Как показали исследования, при непараметрической идентификации трафика в процессе передачи информационных сообщений определяются вид функции распределения и структура (состав) входного информационного потока. На основе полученных результатов принимается решение о принадлежности поступившего трафика к тому или иному классу передаваемого потока данных. Такой подход предварительной оценки поведения трафика в телекоммуникационной сети дает возможность выбора направления дальнейшего исследования и разработки математической модели многопротокольного УС, как основного элемента управления обменом данными в ТКС.

Анализ работ [3-6] показал, что при структурной идентификации трафика используется целый ряд подходов, наиболее результативные из которых базируются на определении передаточных функций по временным и частотным характеристикам информационного потока, идентифика-

ции параметров трафика спектральным методом, а так же идентификации трафика методом корреляции.

Как отмечено в ряде источников [2-3], для моделирования телекоммуникационных систем и идентификации трафика по временным характеристикам широко используются дифференциальные уравнения связи между входными и выходными параметрами информационного трафика:

$$y(t) = pu(t) = \frac{du(t)}{dt} = x^{'}(t),$$

(оператор дифференцирования p),

$$D(y) = \frac{d^n y}{dt^n} + \frac{d^{n-1} y}{dt^{n-1}} + ... + \frac{dy}{dt} + y,$$

(дифференциальный оператор $D(y)$),

$$L(y) = a_n \frac{d^n y}{dt^n} + a_{n-1} \frac{d^{n-1} y}{dt^{n-1}} + ... + a_1 \frac{dy}{dt} + a_0 y,$$

(оператор обыкновенного линейного дифференциального уравнения n-го порядка $L(y)$),

$$y(t) = \int_0^t \omega(t-\tau) u(\tau) d\tau,$$

(линейный интегральный оператор), а так же уравнение связи между входным и выходным сигналами типа интеграла свертки (интеграл Дюамеля):

$$y(t) = \int_0^t x(\tau) w(t-\tau) d\tau = \int_0^t w(\tau) x(t-\tau) d\tau,$$

где $u(t)$ – вектор управления (входа), $y(t)$ – вектор выходных координат объекта, $w(\tau)$ – функция веса объекта управления, т.е. реакция объекта на входной сигнал в виде дельта функции

$$\delta(t) = \begin{cases} 0 \text{ при } t \neq 0 \\ \infty \text{ при } t = 0 \end{cases}; \int_{-\infty}^{\infty} \delta(t) dt = 1.$$

Как показали исследования, дифференциальные уравнения и передаточная функция являются наиболее общими формами связи между переменными состояния на входе и выходе системы. Для уточнения параметров системы (трафика) с помощью эксперимента можно получить данные, определяющие частное решение задачи идентификации. Затем, аппроксимировав аналитическим выражением полученные реализации, можно построить дифференциальное уравнение заданной структуры.

Исследования методов идентификации трафика по временным характеристикам показали, что основным их достоинством является простота реализации и высокая скорость идентификации. Однако ряд их недостатков, связанных, прежде всего с низкой точностью определения характеристик информационного трафика (аппроксимация объекта линейной моделью, используемая в указанных методах снижает точность оценивания при идентификации) и невозможностью учета случайных помех, искажающих реакцию объектов управления, существенно ограничивают практическую реализацию указанных методов при идентификации трафика в ТКС и снижают эффективность использования сетевого оборудования (многопротокольных УС) в процессе передачи данных.

Альтернативой структурной идентификации трафика по временным характеристикам выглядят методы идентификации по частотным характеристикам (частотные методы). В указанных методах, на основе полученных экспериментальным путем данных о поведении трафика в ТКС проводится гармонический частотный анализ. При этом для упрощения процедуры идентификации исследователи ограничиваются вычислением амплитуд и фаз первой и третьей гармоник:

$$b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} y(t) \cos\left(k \frac{2\pi}{T} t \right) dt;$$

$$c_k = \frac{1}{\pi} \int_{-\pi}^{\pi} y(t) \sin\left(k \frac{2\pi}{T} t \right) dt; \qquad (4)$$

$$a_k = \sqrt{b_k^2 + c_k^2};$$

$$\varphi_k = arctg\left(\frac{b_k}{c_k} \right),$$

где T – период колебаний, k – номер гармоники, φ_k – фазовый сдвиг k-ой гармоники.

В том случае если значения выходной величины известны только в дискретные, равноотстоящие моменты времени интегралы в (4) заменяются суммами:

$$b_k = \frac{1}{N} \sum_{i=0}^{N-1} y_i \cos\left(k \frac{ik}{N} \right);$$

$$c_k = \frac{1}{N} \sum_{i=0}^{N-1} y_i \sin\left(k \frac{ik}{N} \right),$$

где N – число отсчетов выходного сигнала.

В результате проведенных операций вычисления амплитуды и фазы входных и выходных гармонических составляющих можно определить значения амплитудно-частотной характеристики на выбранной частоте, как отношение амплитуд гармонических составляющих на выходе и входе объекта управления и значения фазо-частотной характеристики, как фазовый сдвиг φ_k.

Как показали исследования, основным недостатком рассмотренных методов является длительное время эксперимента, затрачиваемое в основном на ожидание установившегося режима при динамических изменениях поведения трафика в ТКС, Кроме того, необходимость в получении достаточного для аппроксимации частотных характеристик количества данных так же приводит к увеличению времени идентификации информационного потока. Поэтому использование методов идентификации по частотным характеристикам трафика в мультисервисных ТКС с динамически изменяемым (флуктуационным)

поведением потока информации существенно затруднено.

Дальнейшим развитием подхода, связанного с идентификацией трафика на основе частотных характеристик, является идентификация информационного потока спектральными методами. Проведенный анализ показал, что указанный вид методов основывается на разложении сигналов по ортонормированным функциям, не обязательно гармоническим. При этом результатом идентификации является определение ядра $h(t,\tau)$ интегрального уравнения объекта, которое в простейшем случае линейных одномерных систем совпадает с функцией веса интегрального уравнения вида:

$$f(t) = y(t) + \int_0^t \bar{h}_y(t,\tau) y(\tau) d\tau , \qquad (5)$$

где $$\bar{h}_y(t,\tau) = \sum_{k=0}^{n-1} \frac{(-1)^k}{(n-1)!} \frac{d^k}{d\tau^k} \left[a_k(\tau)(t-\tau)^{n-1} \right], \qquad (6)$$

$$h(t,\tau) = \begin{cases} \bar{h}(t,\tau), & 0 \le \tau \le t \\ 0, & 0 \le \tau \le T \end{cases} . \qquad (7)$$

Исследования показали, что основным недостатком спектральных методов идентификации трафика является низкая точность оценки исследуемых параметров при наличии посторонних шумов (помех). Так только при наиболее благоприятном случае, когда число обусловленности $K \to 1$ (помеха практически отсутствует) оценка относительной погрешности решения задачи идентификации совпадает с оценкой относительной погрешности исходных данных. В остальных случаях практическое применение спектральных методов идентификации приводит к значительным погрешностям оценки информационного трафика.

Решение указанных проблем идентификации ряд авторов связывают с применением для идентификации трафика корреляционных методов. В этих методах все ненаблюдаемые помехи, воздействующие на различные части объекта исследования (трафика), представляются в виде аддитивного шума, а значение выходного сигнала вычисляется по формуле:

$$y(t) = \int_{-\infty}^{t} \omega(\tau) u(t-\tau) d\tau + e(t) , \qquad (8)$$

где $\omega(t)$ – импульсная переходная характеристика.

В работах [1,3] отмечено, что при выполнении ряда математических операций (интегрирование обоих частей выражения 8 по τ в пределах от $-T$ до T при $T \to \infty$) можно получить выражение:

$$R_{uy}(\tau) = \int_{-\infty}^{\infty} \omega(t) R_{uu}(t-\tau) dt + R_{ue}(\tau) , \qquad (9)$$

где $R_{uu}(\tau)$ – корреляционная функция входного трафика; $R_{uy}(\tau)$ – взаимная корреляционная функция между входным трафиком и выходной последовательностью из системы мультиплексирования; $R_{ue}(\tau)$ – взаимная корреляционная функция между входным трафиком и неуправляемыми сигналами (помехами).

Если $R_{ue}(\tau) = 0$, при $t < 0$ (условие физической реализуемости системы), то уравнение принимает вид:

$$R_{uy}(\tau) = \int_{-\infty}^{\infty} \omega(t) R_{uu}(t-\tau) dt . \qquad (10)$$

Проведенный анализ выражения 10 показал, что оно относится к линейному интегральному уравнению первого рода, а его численное решение осуществляется методом аппроксимирующих функций, вычисление которых, в свою очередь, производится на основе метода коллокации, метода наименьших квадратов и метода Галеркина [1].

Сравнительный анализ методов идентификации трафика показал, что корреляционные методы имеют по сравнению с другими ряд достоинств, таких как простота реализации и высокая скорость идентификации трафика. Однако, как показали исследования, структура уравнения 10 такова, что небольшие ошибки в определении корреляционных функций приводят к существенным ошибкам в определении импульсной переходной характеристики $\omega(t)$ и в итоге к ухудшению точности идентификации параметров трафика.

ВЫВОДЫ

Проведенные сравнительные исследования методов идентификации трафика показали, достоинства (простота реализации, высокая скорость идентификации) корреляционных методов, что позволяет их использовать в процессе управления высокоскоростными информационными потоками в ТКС. Однако выявленные в результате анализа недостатки указанных методов требуют дальнейших исследований и разработки метода структурной идентификации трафика, который наряду с высокой скоростью выполнения необходимых процедур обеспечил максимальную точность идентификации трафика в ТКС.

Литература.

[1] *Городецкий А.Я.* Информационные системы. Вероятностные модели и статистические решения. Учебн. пособие / А.Я.Городецкий СПб: Изд-во СПбГПУ, 2003. 326 с.

[2] *Лагутин В.С., Степанов С.Н.* Телетрафик мультисервесных сетей связи / В.С. Лагутин, С.Н. Степанов. – М.: Радио и связь, 2000. – 320 с.

[3] *Клейнрок Л.* Теория массового обслуживания / Л. Клейнрок. – М.: Машиностроение, 1979. – 432 с.

[4] *Семенов А.Д., Артамонов Д.В., Брюхачев А.В.* Идентификация объектов управления: Учебн. Пособие / А. Д.Семенов, Д. В. Артамонов, А. В. Брюхачев - Пенза: Изд-во Пенз. гос. ун-та, 2003. – 211 с.

[5] *Семенов С.Г.* Анализ методов прогнозирования в

телекоммуникационных сетях автоматизированных систем управления / С.Г.Семенов // Збірник наукових праць «Системи управління, навігації та зв'язку», - К.:ЦНДІ навігації і управління, - 2008.- Вип. 2(6) .- С.134-137

[6] Шелевицький І.В. Методи та засоби сплайн-технології обробки сигналів складної форм / І.В. Шелевицький– Кривий Ріг: Європейський університет, 2002. – 304 с.

Поступила в редколлегию 11.06.2010.

Семенов Сергей Геннадьевич, заместитель начальника информационно-вычислительного центра Харьковского университета воздушных сил имени Ивана Кожедуба

Мелешко Елизавета Владиславовна, аспирант кафедры программного обеспечения, Кировоградский национальный технический университет.

УДК 321.2

Порівняльні дослідження методів ідентифікації трафіку в телекомунікаційній мережі для підвищення оперативності передачі даних / С.Г.Семенов, Є.В.Мелешко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 444-448.

Визначено перспективні напрями підвищення оперативності передачі даних. Проведено порівняйвання дослідження методів ідентифікації трафіку в телекомунікаційній мережі. Представлені математичні моделі систем параметричної та структурної ідентифікації.Виявлено переваги та недоліки різних методів ідентифікації, а так само можливості з використання цих методів для ідентифікації трафіку в телекомунікаційній мережі.Запропоновано шляхи подальших досліджень і розробки методу структурної ідентифікації трафіку для підвищення оперативності передачі даних.

Ключові слова: телекомунікаційні мережі, ідентифікація трафіку, оперативність передачі даних.

Бібліогр.: 06 найм.

UDC 321.2

Comparative study of methods of identifying traffic in a telecommunications network to increase data transmission efficiency/ S.G. Semenov, E.V. Meleshko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 444-448.

Perspective directions of increasing data transmission efficiency are determined. Comparative studies of methods of identifying traffic in a telecommunication network are carried out. Mathematical models of parametric and structural identification are presented. Advantages and disadvantages of different identification methods as well as applicabilities of these methods to traffic identification in a telecommunication network are revealed. Some ways of further research and developments of structural identification method to increase data transmission efficiency are suggestsed.

Key words: telecommunication network, traffic identification, data transmission efficiency.

Ref.: 06 items.

УДК 621.375.826:534.8

ДОСЛІДЖЕННЯ ФАКТОРІВ ВПЛИВУ НА ПОТЕНЦІЙНІ МОЖЛИВОСТІ ЛАЗЕРНИХ СИСТЕМ АКУСТИЧНОЇ РОЗВІДКИ

В.І. ЗАБОЛОТНИЙ, О.Ю. ЄВТУХОВА, Т.М. МАРТИНЕНКО

Дана праця направлена на дослідження особливостей роботи лазерних систем акустичної розвідки (ЛСАР) та визначення факторів, що впливають на їх потенційні можливості і при цьому пов'язані з особливостями конструкції самого приладу. В результаті дослідження створені відповідні якісні та кількісні моделі, що дозволяють оцінювати кількісні характеристики способів та засобів захисту від ЛСАР.

Ключові слова: лазерні системи акустичної розвідки.

ВСТУП

В наш час питання захисту інформації є актуальним та важливим. З розвитком науки створюються нові, все більш ефективні засоби ведення розвідки.

Одним із каналів витоку мовної інформації з приміщень є використання лазерних систем акустичної розвідки (ЛСАР). ЛСАР дозволяє відтворити мову, будь-які інші звуки та акустичні шуми в приміщенні шляхом лазерно-локаційного зондування віконних шибок та інших відбиваючих поверхонь.

Існують кілька схем побудови ЛСАР [1], що забезпечують різну якість розвідування інформації. Найчастіше на практиці використовуються схеми з суміщеним лазером та фотодетектором. Схеми відрізняються в залежності від типу використовуваного лазера, активного середовища. Розрізняють твердотільні, рідкокристаличні, газові і напівпровідникові лазери. Для побудови ЛСАР найчастіше використовують газові та твердотільні лазери.

Для якісного захисту від ЛСАР потрібно враховувати особливості її роботи, в тому числі і чинники, що негативно впливають на якість ведення розвідки. Це дасть змогу знайти її потенційні можливості і на їх основі запропонувати необхідні заходи захисту.

1. ЗАГАЛЬНА МОДЕЛЬ КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ТИПОВОЇ СХЕМИ ЛСАР

Типова схема ЛСАР (рис. 1) заснована на принципі інтерферометра Майкельсона [1]. Принцип роботи даної схеми описується наступним чином: когерентний промінь лазера розчіплюється дільником пучка (сплітером) на 2 частини: опорний промінь та інформаційний. Опорний промінь відбивається від опорного дзеркала і направляється на фотодетектор. При відбиванні інформаційного променя від віконного скла відбувається його модуляція звуковою частотою. Відбитий промодульований промінь направляється на фотодетектор, де інтерферує з опорним променем. Сигнал на фотодетекторі після фільтрації підсилюється і подається для подальшого аналізу.

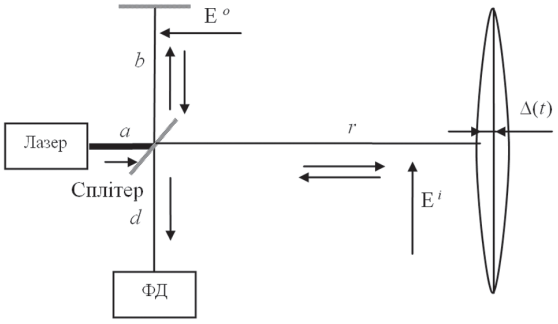


Рис. 1. Типова схема ЛСАР (інтерферометр Майкельсона)

Дана схема створює значну оптичну різницю ходу δ_1 інформаційного та опорного променів

$$\delta_1 = \left(a + 2r + d + 2\Delta(t)\right) - \left(a + 2b + d\right) = 2\left(r + \Delta(t) - b\right). \quad (1)$$

Оптична різниця ходу променів дорівнює:

$$\delta = n_1 \Delta l_1 - n_2 \Delta l_2, \quad (2)$$

де n_1, n_2 – показники заломлення середовищ; Δl_1, Δl_2 – відстані, що проходять промені.

В даному випадку середовище – повітря, тому $n_1 = n_2 = 1$, а $\delta = \Delta l_1 - \Delta l_2$.

Така схема використовується для ЛСАР з газовим лазером. Для використання ЛСАР з твердотільним лазером типова схема повинна бути модифікована з наведених нижче причин.

2. ПРОБЛЕМА МАЛОЇ КОГЕРЕНТНОСТІ ТВЕРДОТІЛЬНИХ ЛАЗЕРІВ

Твердотільні лазери володіють малою в порівнянні з газовими когерентністю. Це пояснюється наступним чином. Часова когерентність визначається часом t_k, на протязі якого випромінювання, випущене з однієї точки джерела, залишається когерентним (наприклад, дає інтерференційну картину на інтерферометрі Майкельсона). Часова когерентність пов'язана з монохроматичністю [2]. Цей зв'язок виражається формулою:

$$t_k = \frac{1}{\Delta\nu}, \quad (3)$$

де $\Delta\nu$ – ширина спектру випромінювання, Гц. Чим менша ширина спектру $\Delta\nu$, тим вище ступінь монохроматичності випромінювання, і тим більша часова когерентність.

Величина оптичної різниці ходу двох хвиль, при якій зберігається їх здатність інтерферувати,

обмежується довжиною когерентності, що обчислюється наступним чином:

$$l_k = t_k \times c, \tag{4}$$

де c – швидкість світла, м/с. Тому для отримання інтерференційної картини на фотодетекторі оптична різниця ходу інформаційного та опорного променів повинна бути меншою за довжину когерентності лазера ($\delta < l_k$).

Твердотільні лазери, на відміну від газових, мають в своєму випромінюванні значний діапазон частот (порівняно велике значення $\Delta\nu$), тобто відрізняються невисокою монохроматичністю.

Взагалі спектр генерації лазерів формується в результаті складної взаємодії між активною речовиною та коливальною системою [3]. Розглянемо основні фактори, що визначають спектр випромінювання лазерів. Перш за все робочий перехід активної речовини характеризується власною шириною лінії, що визначається спонтанним випромінюванням (рис. 2).

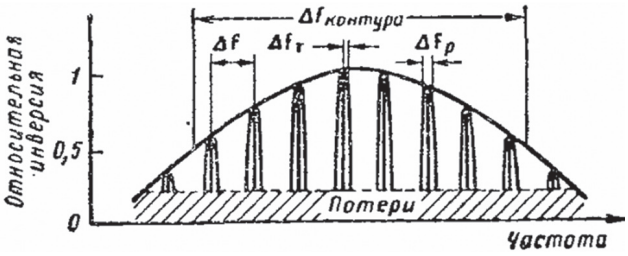


Рис. 2. Спектр випромінювання лазера

В реальних умовах за рахунок різних факторів (ефект Допплера, удари між атомами та молекулами, удари зі стінками) контур лінії розширюється. В межах розширеної лінії розміщуються резонансні лінії резонатора, частоти яких обчислюються за формулою:

$$f_p = \frac{c}{2L \cdot n}. \tag{5}$$

Число резонансних ліній визначається шириною лінії переходу та відстанню між сусідніми піками. Для виготовлення ЛСАР доцільно використовувати лазери, що працюють на одній резонансній частоті, тобто їхній спектр визначається одним резонансним піком.

Ширина резонансного піка визначається добротністю резонатора:

$$\Delta f_p = \frac{f}{Q} = \frac{\alpha c}{2\pi L}. \tag{6}$$

В результаті того, що найбільше посилення активного середовища відбувається в центрі піка резонатора, спектральна лінія випромінювання також розташовується в цьому центрі і має теоретичну ширину:

$$\Delta f_T = \frac{8\pi h f}{P} \Delta f_p^{\,2}. \tag{7}$$

Оскільки частота випромінювання визначається довжиною резонатора, то ширина лінії буде дорівнювати Δf_T, якщо витримувати постійність довжини резонатора з точністю

$$\frac{\Delta L}{L} = \frac{\Delta f_T}{f_T}. \tag{8}$$

Оскільки через механічні та температурні нестабільності таку стабільність довжини резонатора витримати практично неможливо, то дійсна ширина спектра кожної лінії на декілька порядків більша гранично досяжної.

Отже, як видно з формул (3) та (4), широкий спектр випромінювання призводить до зменшення часу когерентності t_k та довжини когерентності l_k, а для отримання чіткої інтерференційної картини бажано забезпечити якомога меншу оптичну різницю ходу інтерферуючих променів ($\delta < l_k$).

Тому для ЛСАР з твердотільним лазером застосовують модифіковану схему – двопроміневу.

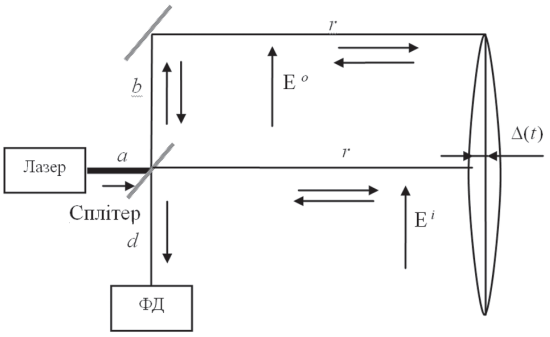


Рис. 3. Двопромінева схема ЛСАР

Відмінність від типової схеми полягає в тому, що опорний промінь направляється на край вікна, і, відбиваючись від нього, спрямовується на фотодетектор. Тоді оптична різниця ходу променів обчислюється наступним чином:

$$\delta_2 = \big(a + 2r + d + 2\Delta(t)\big) - \big(a + 2b + 2r + d\big) = 2\big(\Delta(t) - b\big). \tag{9}$$

Порівняємо оптичні різниці ходу типової і двопроменевої схеми. При порівнянні формул (1) та (9) видно, що $\delta_2 < \delta_1$. Отже, схема, зображена на рис. 3, дозволяє зменшити оптичну різницю ходу променів, що зробить інтерференційну картину, отриману з допомогою твердотільного лазеру, контрастнішою, і як результат, підвищить чутливість приладу.

3. МІНІМІЗАЦІЯ ОПТИЧНОЇ РІЗНИЦІ ХОДУ ІНФОРМАЦІЙНОГО ТА ОПОРНОГО ПРОМЕНІВ

Схему, зображену на рис. 3, можна вдосконалити, звівши оптичну різницю ходу опорного та інформаційного променів до мінімуму. Вдосконалена схема зображена на рис. 4.

Оптична різниця ходу для даної схеми обчислюється наступним чином:

$$\begin{aligned}\delta_3 &= \big(a + 2c + 2b + 2(r - c) + d + 2\Delta(t)\big) - \\ &-\big(a + 2b + 2r + d\big) = a + 2c + 2b + 2r - \\ &-2c + d + 2\Delta(t) - a - 2b - 2r - d = 2\Delta(t).\end{aligned} \tag{10}$$

На схемі, що зображена на рис. 5, КБ – компенсаційний блок. КБ, крізь який проходить інформаційний промінь, призначений для зменшення оптичної різниці ходу між інформаційним

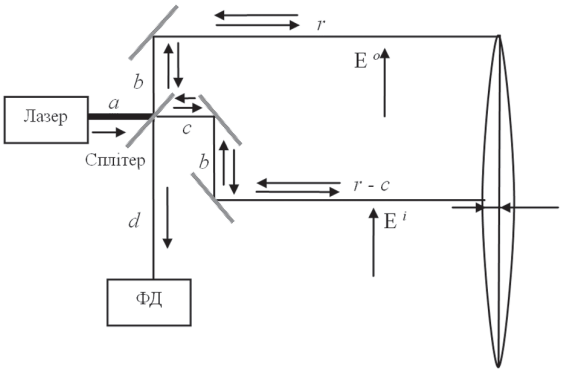


Рис. 4. Схема, що дозволяє зменшити оптичну різницю ходу опорного та інформаційного променів (1 спосіб)

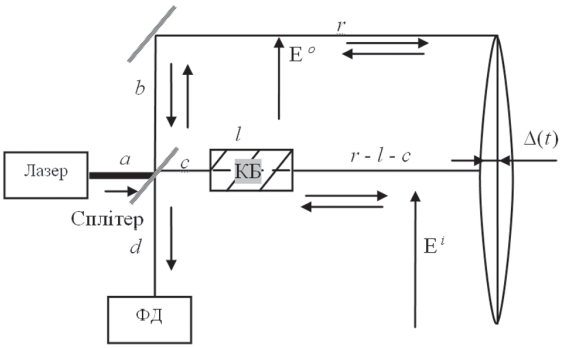


Рис. 5. Схема, що дозволяє зменшити оптичну різницю ходу опорного та інформаційного променів (2 спосіб)

та опорним променем. Він являє собою тіло, протилежні грані якого паралельні, довжиною l, виготовлене з напівпрозорого матеріалу (наприклад, деяке скло), оптична густина n_B якого більша за оптичну густину повітря, тобто $n_B > 1$. Тоді для оптичної різниці ходу справедливе співвідношення (6):

$$\delta_4 = \left(a + 2c + 2b + 2l \cdot n_B + 2(r - l - c) + d + 2\Delta(t)\right) - \\ -\left(a + 2b + 2r + d\right) = 2\left(l \cdot n_B - l + \Delta(t) - b\right). \quad (11)$$

Для отримання чіткої інтерференційної картини бажано забезпечити якомога меншу оптичну різницю ходу інтерферуючих променів, тобто потрібно, щоб $\delta_4 \to 0$. Оскільки $\Delta(t) << l$, $\Delta(t) << b$, то для визначення l величиною $\Delta(t)$ можна знехтувати. Тоді справедливе наступне співвідношення:

$$\delta_4 = 2\left(l \cdot n_B - l - b\right) = 0. \quad (12)$$

Зі співвідношення (7) випливає, що для отримання оптичної різниці ходу близької до нуля, КБ, виготовлений з матеріалу з відомою оптичною густиною n_B повинен мати довжину l, що обчислюється за формулою:

$$l = \frac{b}{n_b - 1}. \quad (13)$$

4. МАТЕМАТИЧНЕ ОБГРУНТУВАННЯ ОПТИМАЛЬНОСТІ ЗАПРОПОНОВАНИХ СХЕМ

Для обгрунтування оптимальності запропонованих схем (рис. 4 та рис. 5) визначимо кореляцію між опорним та інформаційним променем в точці падіння їх на фотодетектор. Чим більш корельованими є промені, тим кращою є якість ведення розвідки. Для визначення кореляції між опорним та інформаційним променем скористаємося теоремою Хінчіна-Вінера [4]:

$$F(\omega) = 2\int_{-\infty}^{\infty} B(\tau)e^{-i\omega\tau}d\tau = 4\int_{0}^{\infty} B(\tau)\cos\omega\tau d\tau, \quad (14)$$

$$B(\tau) = \frac{1}{4\pi}\int_{-\infty}^{\infty} F(\omega)e^{-i\omega\tau}d\omega = \frac{1}{2\pi}\int_{0}^{\infty} F(\omega)\cos\omega\tau d\omega, \quad (15)$$

де $F(\omega)$ – спектральна функція; $B(\tau)$ – функція кореляції; τ – різниця часу проходження відстані до фотодетектора інформаційним та опорним променем; ω – циклічна частота випромінювання лазера, що пов'язана з частотою f співвідношенням

$$\omega = 2\pi f \quad (16)$$

і через власну нестабільність лазера є змінною величиною. Оскільки функція $F(\omega)$ не дорівнює 0 лише на інтервалі $[\omega_p - \Delta\omega_m; \omega_p + \Delta\omega_m]$, то

$$B(\tau) = \frac{1}{2\pi}\int_{0}^{\infty} F(\omega)\cos\omega\tau d\omega = \frac{1}{2\pi}\int_{\omega_@ - \Delta\omega_B}^{\omega_@ + \Delta\omega_B} F(\omega)\cos\omega\tau d\omega. \quad (17)$$

Різниця часу τ визначається наступним чином:

$$\tau = \frac{\delta_4}{c} = \frac{2\Delta(t)}{c}. \quad (18)$$

За приблизними оцінками $\Delta(t) \approx 5$ нм. Тоді

$$\tau \approx \frac{2 \cdot 5 \cdot 10^{-9}}{3 \cdot 10^{8}} \approx 3{,}3 \cdot 10^{-17} \text{ с}. \quad (19)$$

Довжина хвилі лазерів, що використовуються для ЛСАР, може знаходитися між видимим та інфрачервоним випромінюванням. Сучасні лазери працюють на частотах приблизно $3 \cdot 10^{13}$–$5 \cdot 10^{14}$ Гц.

Тоді

$$\cos\omega\tau = \cos\left(2\pi \cdot 3 \cdot 10^{13} \cdot 3{,}3 \cdot 10^{-17}\right) \approx \\ \approx \cos\left(6{,}2 \cdot 10^{-3}\right) \approx 1. \quad (20)$$

Оскільки $\Delta\omega_m$ має невелике значення (в порівнянні з ω_p), то $\cos\omega\tau \approx 1$ на всьому інтервалі $[\omega_p - \Delta\omega_m; \omega_p + \Delta\omega_m]$. Тоді

$$B(\tau) = \frac{1}{2\pi}\int_{\omega_p - \Delta\omega_B}^{\omega_p + \Delta\omega_B} F(\omega)d\omega, \quad (21)$$

тобто при даному значенні τ функція $B(\tau)$ наближається до свого максимального значення і промені при цьому є корельованими, що й треба було довести.

5. НЕРІВНОМІРНИЙ РОЗПОДІЛ НАПРУЖЕНОСТІ МІЖ ІНФОРМАЦІЙНИМ ТА ОПОРНИМ ПРОМЕНЕМ

В загальному випадку, освітленість фотодетектора при інтерференції описується формулою [5]:

$$I(t) \approx (E_o(t) + E_i(t))^2, \quad (22)$$

де $E_o(t)$ – напруженість поля опорного променю, $E_i(t)$ – напруженість поля інформаційного про-

меню. Напруженість поля опорного променю для схеми на рис. 2 представлена наступною формулою:

$$E_o(t) = E_o \sin\varphi_o(t) = E_o \sin(2\pi ft + \\ + k(a + 2b + 2r + d)), \quad (23)$$

а напруженість поля інформаційного сигналу:

$$E_i(t) = E_i \sin\varphi_i(t) = E_i \sin(2\pi ft + \\ + k(a + 2c + 2b + 2(r - c) + d + 2\Delta(t))) = \\ = E_i \sin(2\pi ft + k(a + 2b + 2r + d + 2\Delta(t))). \quad (24)$$

Для ідеального випадку амплітуди світлових векторів $E_o(t)$ та $E_i(t)$ повинні збігатися. Але на практиці амплітуди напруженостей опорного та інформаційного променів не є рівними, тобто $E_o \neq E_i$. Розглянемо як це вплине на сигнал на фотодетекторі. Тоді освітленість фотодетектора виражатиметься формулою:

$$I(t) \approx (E_i(t) + E_o(t))^2 = (E_i \sin(2\pi ft + \\ + k(a + 2b + 2r + d + 2\Delta(t))) + \\ + E_o \sin(2\pi ft + k(a + 2b + 2r + d)))^2 = \\ = (E_i \sin(2\pi ft + kL(t)) + E_o \sin(2\pi ft + kC))^2. \quad (25)$$

Представимо результат у вигляді

$$I(t) \approx E^2(t) = E^2 \cdot \sin^2\varphi(t), \quad (26)$$

де

$$E = \sqrt{E_i^2 + E_o^2 + 2E_iE_o\cos(\varphi_i(t) - \varphi_o(t))} = \\ = \sqrt{E_i^2 + E_o^2 + 2E_iE_o\cos(2\Delta(t))} \quad (27)$$

та

$$\varphi(t) = \operatorname{arctg}\frac{E_i \sin(2\pi ft + kL(t)) + E_o \sin(2\pi ft + kC)}{E_i \cos(2\pi ft + kL(t)) + E_o \cos(2\pi ft + kC)}. \quad (28)$$

Порівняємо графіки сигналів для випадку, коли $E_o = E_i$ та $E_o \neq E_i$ (рис. 6а та 6б).

При порівнянні графіків (рис. 6а та 6б) видно, що при $E_o \neq E_i$ глибина модуляції сигналу звуковою частотою зменшується (огинаюча сигналу на рис. 6б не досягає 0). Чим більша різниця амплітуд E_o та E_i, тим менша глибина модуляції.

На рис. 7 D_m – величина, що показує зменшення глибини модуляції в залежності від відношення E_i до E_o. З графіку видно, що глибина модуляції тим більша, чим ближче до 1 відношення E_i до E_o.

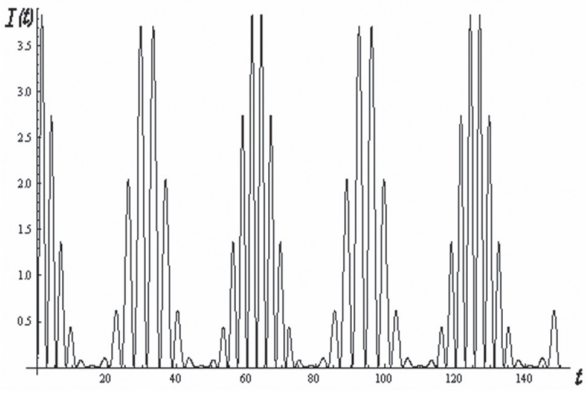


Рис. 6а. Графік сигналу на фотодетекторі при $E_o = E_i$

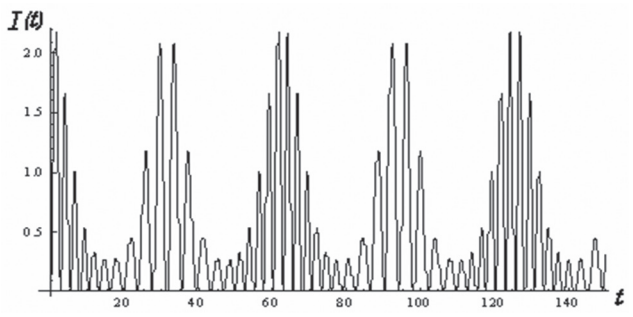


Рис. 6б. Графік сигналу на фотодетекторі при E_o=0,5E_i

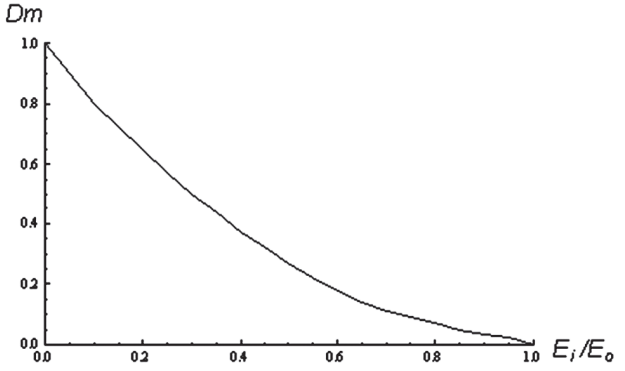


Рис. 7. Графік залежності зменшення глибини модуляції від відношення амплітуд інформаційного та опорного променів

6. ВІДХИЛЕННЯ ОПОРНОГО ПРОМЕНЮ ПРИ КОЛИВАННІ ШИБКИ ВІКНА

При коливанні шибки вікна кут відбивання опорного променю, що падає на край шибки, буде змінюватися, що призведе до відхилення відбитого опорного променя при падінні на опорне дзеркало на деяку відстань z. Кут відхилення залежить від способу закріплення скла в рамі. Розглянемо шарнірне кріплення, при якому кромка пластини під дією звукового тиску може здійснювати обертальний рух уздовж внутрішніх границь рами, що можливо за умови закріплення тільки країв пластини (рис. 8). Вибір даного виду кріплення пластини скла в рамі пояснюється тим, що він забезпечує найбільший кут відхилення променю.

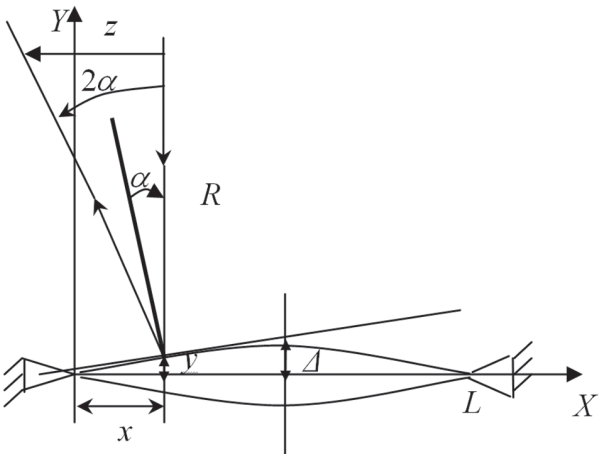


Рис. 8. Відхилення опорного променю при шарнірному кріпленні

При шарнірному кріпленні шибка коливатиметься по закону синуса.

$$y = \Delta_t \sin \pi \frac{x}{L}, \quad (29)$$

$$\Delta_t = \Delta(t) = \Delta \sin w_з t, \quad (30)$$

$$y_{x,t} = \Delta \sin \pi \frac{x}{L} \cdot \sin w_з t, \quad (31)$$

$$tg\alpha = \frac{\partial y'}{\partial x} = \Delta \frac{\pi}{L} \cdot \cos \pi \frac{x}{L} \cdot \sin w_з t \approx \alpha \cdot \sin w_з t, \quad (32)$$

$$z \approx 2R\alpha, \quad (33)$$

$$z_{xt} = 2R \frac{\pi}{L} \cos \pi \frac{x}{L} \cdot \sin w_з t, \quad (34)$$

$$z = 2R \frac{\Delta\pi}{L} \approx 6 \frac{R}{L} \Delta. \quad (35)$$

За приблизними оцінками, амплітуда коливання віконного скла $\Delta \approx 5$ нм. Припустимо, що розвідка ведеться з відстані $R = 50$ м, а вікно, через яке ведеться розвідка, має довжину $L = 1$ м. Тоді

$$z = 6 \cdot \frac{50}{1} \cdot 5 \cdot 10^{-9} = 1{,}5 \cdot 10^{-6} \text{ м}, \quad (36)$$

тобто для вказаних умов ведення розвідки відхилення опорного променя $z \approx 1{,}5$ мкм і є замалим для створення відчутних завад.

ВИСНОВКИ

Отже, в даній статті були розглянуті фактори, що негативно впливають на якість ведення розвідки за допомогою ЛСАР. До таких факторів належать нерівномірний розподіл напруженості між інформаційним та опорним променями, відхилення опорного променю при коливанні шибки вікна та мала когерентність випромінювання при використанні твердотільного лазеру. Проаналізовані і запропоновані схеми (рис. 4 та рис. 5), що вирішують проблему зменшення оптичної різниці ходу інформаційного та опорного променю, зводячи її до мінімуму і таким чином знижують вплив малої когерентності на якість прийнятого сигналу.

Створені окремі моделі, вибором яких можна створювати найкращі потенційні можливості ЛСАР для відповідних умов їх використання, дозволяють оцінювати кількісні характеристики способів та засобів захисту від ЛСАР.

Література.

[1] Laser microphone – http://www.williamson-labs.com/laser-mic.htm

[2] *Сэм М.Ф.* Лазеры и их применение// Соросовский образовательный журнал – 1996 . – № 6

[3] Справочник по радиоэлектронике в трех томах / Куликовский А. А. – Том 3, М.: «Энергия», 1970 –816 с.

[4] *Левин Б.Р.* Теоретические основы статистической радиотехники. Книга первая – М.: «Советское радио», 1969. – 752 с.

[5] *Малашин М.С.* Основы проектирования лазерных локационных систем : учеб. пособие / М.С. Малашин, Р.П. Каминский, Ю.Б. Борисов. – М.: «Высшая школа», 1983. – 207 с.

Надійшла до редколегії 17.06.2010.

Заболотний Володимир Ілліч, канд. техн. наук, доцент кафедри БІТ ХНУРЕ. Область наукових інтересів: технічний захист інформації.

Євтухова Ольга Юріївна, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: технічний захист інформації.

Мартиненко Тетяна Михайлівна, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: технічний захист інформації.

УДК 621.375.826:534.8

Исследование факторов влияния на потенциальные возможности лазерных систем акустической разведки / В.И. Заболотный, О.Ю. Евтухова, Т.М. Мартыненко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 449–453.

В статье были проведены исследование особенностей работы лазерных систем акустической разведки (ЛСАР) и определены факторы, влияющие на их потенциальные возможности и при этом связанные с особенностями конструкции самого прибора. В результате исследования созданы соответствующие качественные и количественные модели, позволяющие оценивать количественные характеристики способов и средств защиты от ЛСАР.

Ключевые слова: лазерные системы акустической разведки.

Ил. 08. Библиогр.: 05 назв.

UDC 621.375.826:534.8

Investigation of factors influencing the potential of laser systems of acoustic intelligence / V.I. Zabolotny, O.Yu. Etukhova, T.M. Martynenko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 449-453.

The paper is devoted to researching operation features of laser systems of acoustic intelligence (LSAI) and defining factors which influence their potential possibilities and which are connected with features of the design of the device itself. As a result of the research appropriate qualitative and quantitative models are created which allow to estimate the quantitative characteristics of ways and means for protection against LSAIs.

Key words: laser systems of acoustic intelligence.

Fig. 08. Ref.: 05 items.

УДК 681.3:681.04

МЕТОД СНИЖЕНИЯ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ РЕАЛИЗАЦИИ RSA КРИПТОПРЕОБРАЗОВАНИЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПРИНЦИПА КОЛЬЦЕВОГО СДВИГА В МОДУЛЯРНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

С.О. МАРТЫНЕНКО, В.А. КРАСНОБАЕВ, А.А. ЗАМУЛА, О.М. ХАЛИНА

В статье рассматривается метод аппаратной реализации арифметической модульной операции умножения в спецпроцессоре обработки криптографической информации (СОКИ). Метод основан на принципе кольцевого сдвига в модулярной системе счисления (МСС). Использование МСС позволяет эффективно, с точки зрения повышения быстродействия реализации криптографических преобразований, организовать процесс реализации модульной целочисленной арифметической операций умножения. Разработанный метод рекомендован к использованию в СОКИ при реализации криптографических RSA преобразований.

Ключевые слова: спецпроцессор обработки криптографической информации, модулярная система счисления.

ВВЕДЕНИЕ

Система RSA, входящая в стандарт X-509, широко используется в современных криптосистемах для реализации цифровой подписи и несимметричного шифрования. Основными операциями при реализации вычислений и проверки цифровой подписи являются операции модульного умножения и операция возведение чисел в квадрат по модулю [1-4]. Современные спецпроцессоры обработки криптографической информации (СОКИ) при реализации криптопреобразований с открытым ключом значительную часть времени тратят на реализацию операции модульного умножения. Так, если размерность обрабатываемых чисел равна m, то для RSA-криптопреобразований количество операций модульного умножения и операций возведения чисел в квадрат по модулю, выполняемых СОКИ, равно, соответственно, $m/2$ и m.

Известно, что вычислительная сложность (ВС) криптографического алгоритма определяется временем его реализации. В общем случае ВС определяется количеством входящих в алгоритм разнотипных операций и временем реализации каждой из операции. Таким образом, существуют два пути снижения ВС реализации алгоритма: частичное сокращение количества операций и уменьшение времени реализации операций. Первый путь предполагает изменение алгоритма, что вряд ли целесообразно и вообще возможно. Второй путь - основан на уменьшении времени выполнения модульных операций, которые в современных СОКИ (embedded processor, processor node) реализуются в обычной двоичной позиционной системе счисления (ПСС).

ОСНОВНАЯ ЧАСТЬ

Проведенные исследования показали, что двоичная ПСС, в которой представляется и обрабатывается информация в современных СОКИ, обладают существенным недостатком – наличием межразрядных связей. Данный недостаток накладывают свой отпечаток на методы реализации арифметических операций, усложняют аппаратуру, снижает достоверность вычислений, и ограничивают быстродействие реализации криптографических преобразований. Поэтому естественно изыскание возможностей построения такой арифметики, в которой бы поразрядные связи отсутствовали. В этом плане обращает на себя внимание модулярная система счисления (МСС). МСС обладает ценным свойством независимости друг от друга остатков по принятой системе оснований. Эта независимость открывает широкие возможности в построении не только новой машинной арифметики, но и принципиально новой схемной реализации СОКИ, которая в свою очередь заметно расширяет применение этой машинной арифметики. Во многих литературных источниках отмечается, что одним из практических направлений повышения пользовательской производительности вычислительных средств является внедрение нетрадиционных методов представления и параллельной обработки информации в числовых системах с параллельной структурой. В частности, в МСС, обладающих максимальным уровнем внутреннего параллелизма в организации процесса переработки информации [5, 6].

Цель статьи – разработка метода снижения вычислительной сложности RSA криптопреобразований на основе использования принципа кольцевого сдвига в модулярной системе счисления. В этом случае снижение вычислительной сложности RSA систем основано на использовании второго пути – уменьшения времени выполнения операций, входящих в алгоритмы криптопреобразований. В частности, уменьшение времени реализации операции модульного умножения.

Для исследования методов выполнения операции модульного умножения в МСС, на основе использования ПКС, введем и воспользуемся понятием оператора кольцевого сдвига (ОКС). ОКС – это оператор, определяющий величину (выраженную в количестве z одновременно

сдвигаемых разрядов КСР) и направление сдвига разрядов КСР при реализации арифметических операций и обозначается как $k^{(z)}$, где

$$z=\begin{cases}+z, & \text{при положительном направлении сдвига содержимого разрядов КСР,}\\ -z, & \text{при отрицательном (по часовой стрелке направлении сдвига содержимого разрядов КСР),}\end{cases}$$

а z – показатель оператора кольцевого сдвига (ПОКС).

Метод реализации операции модульного умножения $a_i \cdot \beta_i \pmod{m_n}$ на основе ПКС состоит в использовании набора из двух КСР с применением известного соотношения:

$$a_i\beta_i \pmod{m_n} = \left[\left\{(a_i+\beta_i)\bmod m_n\right]^2 \bmod m_n - \right.$$
$$\left. -\left[(a_i-\beta_i)\bmod m_n\right]^2 \bmod m_n\right\}\bmod m_n)/4\Big]\bmod m_n. \quad (1)$$

В этом случае ОКС для первого КСР представится в виде $k^{(+\beta_i)}$, а для второго – $k^{(-\beta_i)}$. Время t выполнения операции модульного умножения будет не намного больше того времени, что определяется выражением для сложения-вычитания [7, 8]. Недостаток данного варианта реализации операции модульного умножения – сравнительно большой объем оборудования операционного устройства СОКИ.

Рассмотрим предлагаемый в статье метод реализации операции модульного умножения, основанного на использовании двоичного представлении остатков числа в МСС [9]. Назовем разработанный метод для операции целочисленного модульного умножения – метод контуров (МК). В этом случае используется всего один КСР, с помощью которого определяется результат операций модульного сложения, вычитания и умножения. Для операции модульного умножения ОКС представляется в виде $K_{ij}^{(z_i)}$, где i – номер контура, в котором производится сдвиг содержимого разрядов КСР ($i=\overline{1,n}$); $n=m_n-1$ – количество контуров, по которым работает устройство; j – номер устанавливаемой строки матрицы значений $a\cdot\beta \pmod{m_n}$ (индекс i для операндов a и β опускается), $j=\overline{1,n}$; z_i – ПОКС, обозначающий количество сдвигов содержимого разрядов КСР в данном i-м контуре $\left(z_i=\overline{0,m_i-2}\right)$.

Сущность МК состоит в том, что по значению второго β операнда устанавливается β-я строка таблицы значений $a\cdot\beta \pmod{m_n}$ путем сдвига содержимого разрядов КСР по отдельным контурам (по отдельным модулям m_i, причем $m_i=i+1$, так как минимальный (первый) модуль равен двум, т.е. $m_i=2$. Поскольку нулевая строка таблицы значений $a\ \beta \pmod{m_n}$ не устанавливается ($j\neq 0$), то $j=\overline{2,n}$. Вместе с тем первый разряд КСР устанавливается одновременно со вторым и, таким образом, $i=\overline{2,n}$. Нулевой разряд КСР участия в реализации МК не принимает, так как операция умножения на ноль (a=0; β=0) проще организуется по отдельному алгоритму, например, путем вывода входных нулевых шин операндов a, β непосредственно на нулевой выход устройства. Установление значения содержимого разрядов КСР производится последовательно, начиная с (m–1)-го (старшего) разряда и до второго включительно, т.е. справа налево (табл. 1). На рис. 1 представлена схема реализации операции модульного умножения для произвольного модуля m_i МСС, а на рис. 2 представлена схема реализации операции модульного умножения для модуля $m_i=5$.

Таблица 1

Исходные данные для реализации операции модульного умножения в МСС

β_i	a_i				
	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Введем понятие обобщенного операнда кольцевого сдвига (ООКС) в виде матрицы $\left\{K_{ij}\right\}=\left\{K_{ij}^{(z_{ij})}\right\}$, где показатель обобщенного операнда кольцевого сдвига (ПООКС) z_{ij} означает количество сдвигов содержимого разрядов КСР в i-м контуре при установлении j-й строки матрицы модульного произведения $a\cdot\beta \pmod{m_n}$. Таким образом, ООКС $\{K_{ij}\}$ будет состоять из набора (m_n-2)-х ОКС и может быть разложен либо по строкам $K_j\left(j=\overline{2,n}\right)$, либо по контурам $K\left(i=\overline{2,n}\right)$ в виде

$$\left\{K_{ij}\right\}=K_j=\left(K_{2j}^{(z_{2j})}K_{3j}^{(z_{3j})}\ \ldots\ K_{nj}^{(z_{nj})}\right), \quad (2)$$

$$\left\{K_{ij}\right\}=K_i=\left(K_{i2}^{(z_{i2})}K_{i3}^{(z_{i3})}\ \ldots\ K_{in}^{(z_{in})}\right). \quad (3)$$

Исходя из записи ООКС $\{K_{ij}\}$ (2), можно определить временную матрицу $\{T_j\}$:

$$\left\{T_j\right\}=\begin{vmatrix} z_{22} & z_{32} & \ldots & z_{n2}\\ \vdots & \vdots & & \vdots\\ z_{2n} & z_{3n} & \ldots & z_{nn}\end{vmatrix}. \quad (4)$$

Время t_j установления j-й строки матрицы (время реализации операции) значений $a\ \beta \pmod{m_n}$ равно сумме ПООКС для j-й строки матрицы (4), умноженной на величину

$$k\cdot\tau, \quad (5)$$

т.е.

$$t_j=\sum_{i=2}^{n} z_{ij}k\tau\,. \quad (6)$$

Очевидно, что $t\approx t_j$. Время t реализации модульной операции умножения можно так же определить, исходя из выражения (3). Действительно, в этом случае временная матрица $\{T_i\}$ по контурам будет совпадать с транспонированной матрицей $\left\{T_j\right\}$, т.е. определить, исходя из выра-

жения (3). Действительно, в этом случае временная матрица $\{T_i\}$ по контурам будет совпадать с транспонированной матрицей $\{T_j\}$, т.е.

$$\{T_i\}=\{T_j\}^T=\begin{vmatrix} z_{22} & z_{23} & \dots & z_{2n} \\ \vdots & \vdots & & \vdots \\ z_{n2} & z_{n3} & \dots & z_{nn} \end{vmatrix}, \qquad (7)$$

а время установления j-й строки матрицы равно сумме ПООКС для j-го столбца матрицы (7), умноженной на величину $k\tau$. Очевидно, что в общем случае время t реализации модульной операции $a\beta(\mathrm{mod}\ m_n)$ как и для операции модульного сложения и вычитания, зависит от величины операнда β (от номера j устанавливаемой строки), т.е.

$$t_{j\,\min} \le t \le t_{j\,\max}. \qquad (8)$$

Исходя из выражения (8), целесообразно оперировать средним $t_{\text{ср}}$ и максимальным $t_{\max}$ временем реализации модульных операций

$$t_{\max}^{(x)} = \sum_{i=2}^{n} t_{ij\ \max}, \qquad (9)$$

$$t_{\text{ср}}^{(x)} = \sum_{i=2}^{n} t_{ij\ \max}/(n-1). \qquad (10)$$

В соответствии с выражением (6) запишем формулы (9), (10) в следующем виде

$$t_{\max}^{(x)} = k\tau\cdot(m_n-1)m_n/2, \qquad (11)$$

$$t_{\text{ср}}^{(x)} = k\tau\sum_{i=2}^{n}(m_i-2)/2. \qquad (12)$$

Отметим, что в каждом из контуров можно применить разработанные алгоритмы сокращения времени установления нужной строки таблицы, которая реализует соответствующую модульную операцию [7]. В этом случае, результат операции модульного умножения будет определяться за время меньшее, чем то, что определяется выражениями (6)–(12). Известно [8], что время реализации операций сложения $t_{\text{слож}}$ и умножения $t_{\text{умн}}$ в ПСС определяться следующими выражениями:

$$t_{\text{слож}} = \tau + (\rho-1)(\tau_{\text{и}} + \tau_{\text{или}} + \tau), \qquad (13)$$

$$t_{\text{умн}} = \rho(\tau + t_{\text{слож}}), \qquad (14)$$

где: ρ – количество двоичных разрядов в представлении операндов (разрядная сетка СОКИ); $\tau_{\text{и}}$ ($\tau_{\text{или}}$) – время прохождения сигнала через эле-

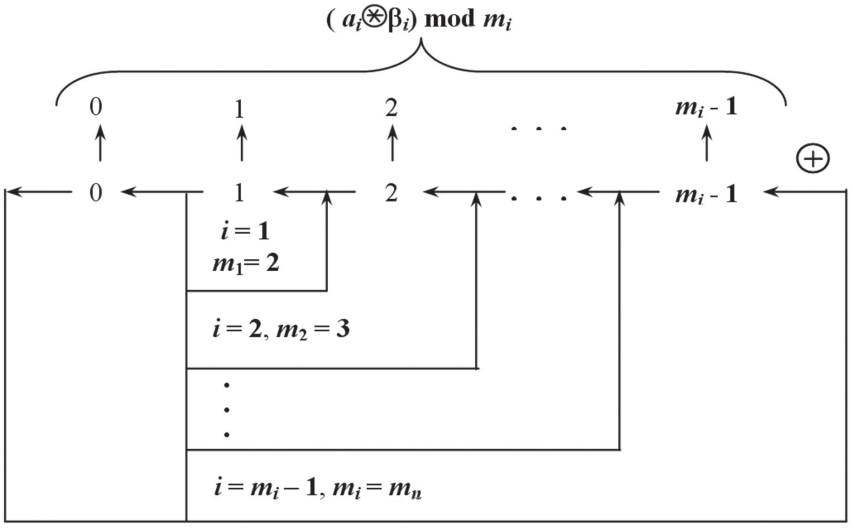


Рис. 1. Схема реализации операции модульного умножения для произвольного модуля mi МСС

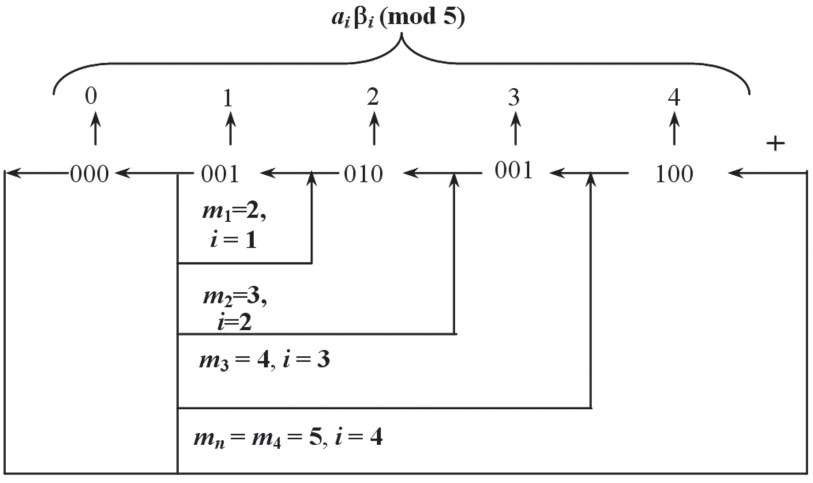


Рис. 2. Схема реализации операции модульного умножения для $m_i = 5$

мент И (ИЛИ) (время «срабатывания» соответствующего логического элемента, т.е. одного вентиля). Принимая во внимание, что $\tau_{и} \approx \tau_{или} \approx \tau/2$, запишем выражения (13) и (14) в виде

$$t_{слож} = \tau\,(2\rho - 1), \qquad (15)$$

$$t_{умн} = 2\tau\rho^2. \qquad (16)$$

Рассмотрим пример технической реализации операции модульного умножения в МСС для $m_n = 5$ (табл. 2). В соответствии с выражениями (2) и (3) ООКС для $m_n = 5$ представим в виде

$$\left\{K_{ij}\right\} = \left\{K_{2j}^{z_{2j}} K_{3j}^{z_{3j}} K_{4j}^{z_{4j}}\right\}. \qquad (17)$$

Разложим ООКС по строкам и контурам.

По строкам получим:

$$j = 2,\ K_2 = \left\{K_{22}^{z_{22}} K_{32}^{z_{32}} K_{42}^{z_{42}}\right\},$$

$$j = 3,\ K_3 = \left\{K_{23}^{z_{23}} K_{33}^{z_{33}} K_{43}^{z_{43}}\right\},$$

$$j = 4,\ K_4 = \left\{K_{24}^{z_{24}} K_{34}^{z_{34}} K_{44}^{z_{44}}\right\}.$$

По контурам имеем:

$$i = 2,\ K_2 = \left\{K_{22}^{z_{22}} K_{23}^{z_{23}} K_{24}^{z_{24}}\right\},$$

$$i = 3,\ K_3 = \left\{K_{32}^{z_{32}} K_{33}^{z_{33}} K_{34}^{z_{34}}\right\},$$

$$j = 4,\ K_4 = \left\{K_{42}^{z_{42}} K_{43}^{z_{43}} K_{44}^{z_{44}}\right\}.$$

На основании соотношения (17) ООКС для соответственно второй ($j = 2$), третьей ($j = 3$) и четвертой ($j = 4$) строк табл. 1 будет иметь следующий вид:

$$K_2 = \left\{K_{22}^{(0)} K_{32}^{(2)} K_{42}^{(3)}\right\},$$

$$K_3 = \left\{K_{23}^{(1)} K_{33}^{(2)} K_{43}^{(2)}\right\},$$

$$K_4 = \left\{K_{24}^{(1)} K_{34}^{(1)} K_{44}^{(1)}\right\}.$$

Общий алгоритм образования ПОКС и ООКС для $m_n = 5$ представлен в табл. 2 (см. рис. 2). Определим время t_j установления j-й строки табл. 1 в соответствии с выражением (6): $t_2 = 15\,\tau$, $t_3 = 15\,\tau$, $t_4 = 9\,\tau$ ($k = [\log_2(m_n - 1)] + 1 = 3$). Отметим, что в соответствии с выражением (14) максимальное время установления j-й строки равно $t_{\max}^{(x)} = 30\tau$ ($t_{ср}^{(x)} = 13{,}5\tau$). Данное обстоятельство подтверждает, что реальная эффективность применения ПКС в МСС выше, чем та, что определяется выражениями (11) и (12).

На рис. 3 и 4 представлены упрощенные варианты схем функционирования операционных устройств СОКИ в МСС при использовании ПКС.

Таблица 2

Алгоритмы образования ПОКС и ООКС для $m_n = 5$

Номер устанавливаемой строки матрицы $j = \beta = \overline{2,4}$	Номер контура $i = \overline{2,4}$	ПОКС $z_{i,j}$	Исходное содержимое КСР	ОКС (z_i) $K_{i,j}$	ООКС $\{K_{i,j}\}$
$j = 2$	$i = 4$	$z_{42} = 3$	0 2 3 4 1 0 3 4 1 2 0 4 1 2 3	$K_{42}^{(3)}$	$K_2 = \left\{K_{22}^{(0)} K_{32}^{(2)} K_{42}^{(3)}\right\}$
	$i = 3$	$z_{32} = 2$	0 1 2 4 3 0 2 4 1 3	$K_{32}^{(2)}$	
	$i = 2$	$z_{22} = 0$	0 2 4 1 3	$K_{22}^{(6)}$	
$j = 3$	$i = 4$	$z_{43} = 2$	0 2 3 4 1 0 3 4 1 2	$K_{43}^{(2)}$	$K_3 = \left\{K_{23}^{(1)} K_{33}^{(2)} K_{43}^{(2)}\right\}$
	$i = 3$	$z_{33} = 2$	0 4 1 3 2 0 1 3 4 2	$K_{33}^{(2)}$	
	$i = 2$	$z_{23} = 1$	0 3 1 4 2	$K_{23}^{(1)}$	
$j = 4$	$i = 4$	$z_{44} = 1$	0 2 3 4 1	$K_{44}^{(1)}$	$K_4 = \left\{K_{24}^{(1)} K_{34}^{(1)} K_{44}^{(1)}\right\}$
	$i = 3$	$z_{34} = 1$	0 3 4 2 1	$K_{34}^{(1)}$	
	$i = 2$	$z_{24} = 1$	0 4 3 2 1	$K_{24}^{(1)}$	

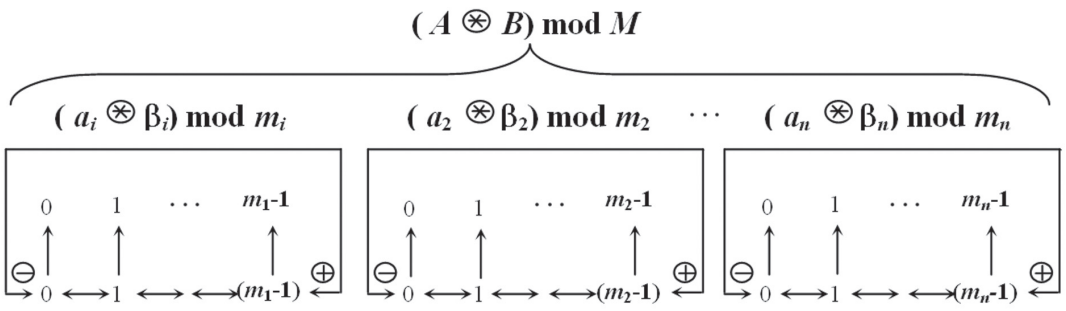


Рис. 3. Операционного устройства СОКИ в МСС

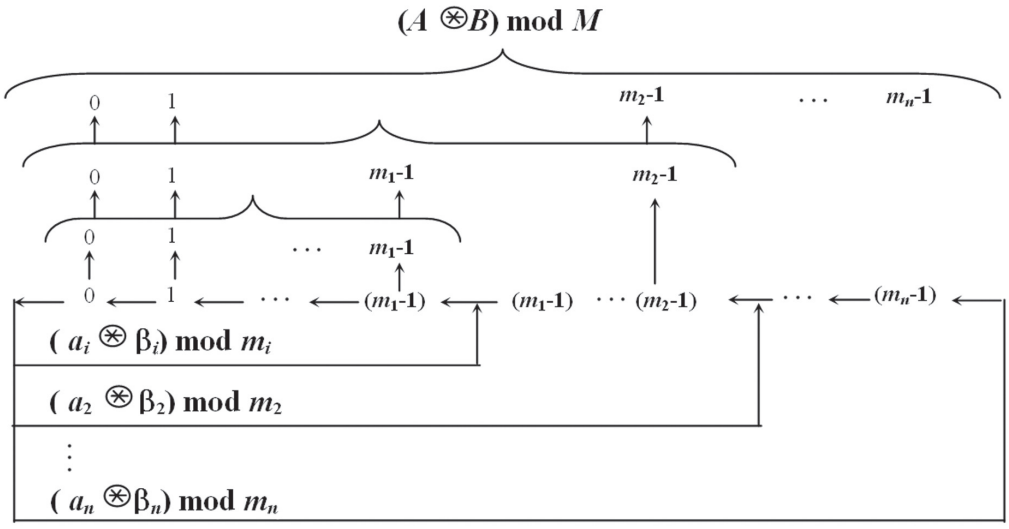


Рис. 4. Операционного устройства СОКИ в МСС

ВЫВОДЫ

В статье предложен метод уменьшения вычислительной сложности реализации алгоритмов RSA на основе использования ПКС в МСС. На основании данного метода разработаны алгоритмы его реализации, а также структуры операционных устройств СОКИ в МСС. Проведенный расчет времени реализации арифметической операции модульного умножения, даже без учета влияний алгоритмов повышения быстродействия, показал высокую эффективность использования предложенного метода. Разработанный метод, алгоритмы и структуры могут быть рекомендованы к практическому использованию для снижения вычислительной сложности реализации криптопреобразований в СОКИ.

Литература.

[1] *Е.Г. Качко, С.С. Батюшко.* Оптимизация алгоритмов для современных стандартов метода RSA // Прикладная радиоэлектроника. Научно-технический журнал. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – Том 7. 2008. № 3. – С. 252-255.

[2] *Грайворонський М.В., Новіков О.М.* Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

[3] *Шнайер Б.* Прикладная криптография. – М.: Издво. «Триумф», 2002. – 797 с.

[4] *Горбенко И.Д., Збитнев С.И., Поляков А.А.* Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда // Радиотехника: Всеукр. межвед. научн-тех. сб. 2001. Вып. 119. – С. 43-50.

[5] *V.A. Krasnobayev.* Method for Realization of Transformations in Public-Key Cryptography, Telecommunications and Radio Engineering (USA), 2007, Vol. 66, Issue 17, pp. 1559-1572.

[6] *Барсов В.И., Сорока Л.С., Краснобаев В.А., Хери Али Абдуллах.* Модели и методы повышения отказоустойчивости и производительности управляющих вычислительных комплексов специализированных систем управления реального времени на основе применения непозиционных кодовых структур модулярной арифметики. Монография. – Х.: УИПА, 2008. – 147 с.

[7] *Барсов В.И., Сорока Л.С., Краснобаев В.А.* Методология параллельной обработки информации в модулярной системе счисления: Монография. – Х.: МОН, УИПА, 2009. – 268 с.

[8] *В. А. Краснобаев, С.О. Мартыненко, Ж.В. Дейнеко, А.А. Замула, А.А. Баклыков.* Метод обработки криптографической информации в модулярной системе счисления, основанный на принципе кольцевого сдвига // Прикладная радиоэлектроника. Научно-технический журнал. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – Том 8. 2009. № 3. – С. 343-350.

[9] *Есин В.И., Кузнецов А.А., Сорока Л.С.* Безопасность информационных систем и технологий. – Харьков. ООО “ЭДЭНА”, 2010. – 656 с.

Поступила в редколлегию 21.06.2010.

Мартыненко Сергей Олегович, руководитель предприятия, г. Харьков. Область научных интересов: создание систем быстрой обработки криптографической информации в реальном времени на основе кодов модулярной системы счисления.

Краснобаев Виктор Анатольевич, профессор кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенко, доктор техн. наук, профессор, Заслуженный изобретатель Украины, Почётный радист СССР. Область научных интересов: теоретическое обоснование и практическое создание сверхбыстродействующих и высокоотказоустойчивых вычислительных структур в модулярной арифметике.

Замула Александр Андреевич, профессор кафедры БИТ ХНУРЭ, канд. техн. наук, доцент. Область научных интересов: технологии защиты информации в информационно-телекоммуникационных системах.

Халина Ольга Михайловна, инженер ЗАО «ИИТ». Область научных интересов: защита информации в информационно-телекомуникационных системах.

УДК 681.3:681.04

Метод зниження обчислювальної складності реалізації RSA криптоперетворень на основі використання принципу кільцевого зсуву в медулярній системі числення / С. О. Мартиненко, В. А. Краснобаєв, О.А. Замула, О.М. Халіна // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 454-459.

В статті розглядається метод апаратної реалізації арифметичної модульної операції множення у спец процесорі обробки криптографічної інформації (СОКІ). Метод заснований на принципі кільцевого зсуву в модулярній системі числення (МСЧ). Використання МСЧ дозволяє ефективно, з точки зору підвищення швидкодії реалізації криптографічних перетворень, організувати процес реалізації модульної цілочисельної арифметичної операції множення. Розроблений метод рекомендований до використання в СОКІ при реалізації криптографічних RSA перетворень.

Ключові слова: спецпроцесор обробки криптографічної інформації, модулярная система числення.

Табл. 02. Іл.04. Бібліогр.: 09 найм.

UDC 681.3:681.04

Method of reducing computational complexity for realizing RSA cryptotransformations on the basis of using the principle of circular shift in the modular number system / C.O. Martynenko, V.A. Krasnobaev, A.A. Zamula, O.M. Halina // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 454-459.

The paper considers the method of hardware implementation of an arithmetic modular multiplication operation in a special processor of cryptographic information processing (SPCIP). The method is based on the principle of circular shift in modular number system (MNS). The use of MNS allows effectively, from the point of view of increasing the speed of realizing cryptographic transformations, to organize the process of realizing a modular arithmetic multiplication operation. The developed method is recommended to be used in a SPCIP during realization of cryptographic RSA transformations.

Key words: special processor for cryptographic information processing, modular system of notation.

Tab. 02. Fig. 04. Ref.: 09 items.

УДК 004.056.5

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

Розглядається порядок здійснення заходів та засобів при створенні комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах.

Ключові слова: комплексні системи захисту інформації, інформаційно-телекомунікаційні системи.

ВСТУП

Забезпечення безпеки інформації у інформаційно-телекомунікаційних системах здійснюється шляхом створення та впровадження комплексних систем захисту інформації.

Комплексна система захисту інформації (рис. 1) – це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації від несанкціонованого доступу.

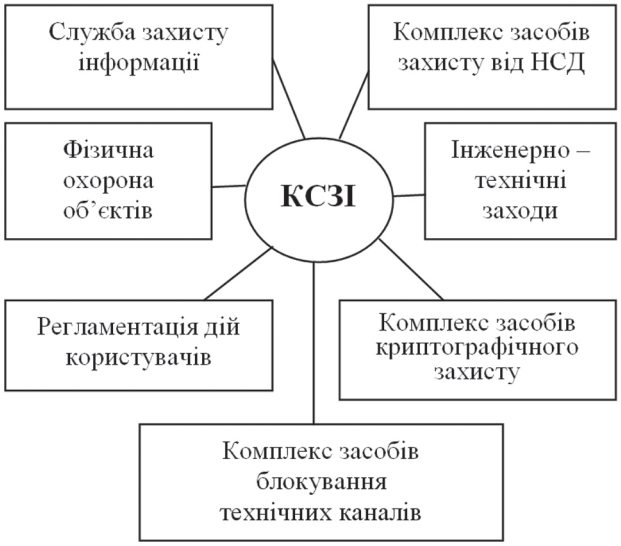


Рис. 1. Комплексна система захисту інформації

1. ПРАВОВІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

В Законі України «Про захист інформації в інформаційно-телекомунікаційних системах визначено: «Інформація, яка є власністю держави або інформація з обмеженим доступом, вимога щодо якості якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (далі – КСЗІ) з підтвердженою відповідністю». В зазначеному Законі КСЗІ розглядається як взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [1].

Захист інформації є складовою частиною робіт зі створення та експлуатації інформаційно-телекомунікаційних систем (далі – ІТС) і повинен здійснюватися на всіх етапах життєвого циклу ІТС. У ряді чинних нормативно-правових документах визначається, що захист інформації в ІТС забезпечується:

– впровадженням комплексної системи захисту інформації;

– дотриманням суб'єктами відносин, пов'язаних з обробкою інформації в ІТС, законодавства України та нормативних документів у сфері захисту інформації;

– використанням засобів електронно-обчислювальної техніки, програмного забезпечення, телекомунікаційного обладнання, а також засобів захисту інформації, які відповідають вимогам законодавства України щодо захисту інформації.

2. ПОРЯДОК СТВОРЕННЯ КСЗІ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Роботи зі створення КСЗІ виконуються організацією-власником ІТС. За умови відсутності у неї відповідних ліцензій або дозволу на здійснення окремих видів робіт із захисту інформації до виконання цих робіт залучаються суб'єкти господарювання, які мають такі ліцензії. Дозвіл на проведення робіт з технічного захисту інформації (далі – ТЗІ) для власних потреб дається Державною службою спеціального зв'язку та захисту інформації (далі – ДССЗЗІ) України у порядку, який визначено Положенням про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. [2]

КСЗІ розробляється і впроваджується в ІТС, що створюються, а також у діючих ІТС, якщо виникла необхідність забезпечення в них захисту інформації.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розробку і впровадження інформаційної технології, що забезпечує обробку інформації в ІТС згідно з вимогами, встановленими державними стандартами, нормативно-правовими актами та нормативними документами у сфері захисту інформації.

Комплексна система захисту інформації є невід'ємною складовою частиною автоматизованої системи (далі – АС) і на неї поширюються всі вимоги державних стандартів щодо створення АС.

Для створення КСЗІ використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок

за результатами державної експертизи у сфері технічного та криптографічного захисту інформації.

2.1. Послідовність робіт зі створення КСЗІ

Нормативними документами в сфері ТЗІ визначений порядок проведення робіт зі створення КСЗІ. Основними етапами створення КСЗІ є:

– формування служби захисту інформації (призначення відповідальної особи) для організації робіт зі створення КСЗІ, її експлуатації та контролю за станом захищеності інформації;

– обстеження умов функціонування ІТС та розробка технічного завдання на створення КСЗІ;

– розробка та реалізація проекту КСЗІ;

– введення КСЗІ в дію та оцінка захищеності інформаційних ресурсів ІТС. [2]

Стадії та етапи робіт, які виконуються під час створення КСЗІ в конкретній ІТС, їх зміст і результати, терміни виконання визначаються технічним завданням на створення КСЗІ та договорами між замовником і виконавцями робіт.

Вимоги щодо захисту інформації, які реалізуються КСЗІ, визначаються необхідним рівнем забезпечення властивостей, що характеризують захищеність інформації: цілісність, конфіденційність, доступність.

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 і наведень, акустоелектричні та інші канали;

– несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування 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.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються рівнем критичності оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС відповідно до нормативних документів з захисту інформації.

Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, яка становить державну таємницю або коли необхідність цього визначена власником інформації.

Створення комплексу засобів захисту(далі – КЗЗ) інформації від несанкціонованого доступу (далі – НСД) здійснюється у всіх ІТС, де обробляється інформація, яка є власністю держави або що відноситься до державної таємниці, або до окремих видів інформації, захист яких гарантується державою, а також в ІТС, де така необхідність визначена власником інформації.

Порядок розробки, впровадження, використання у складі КСЗІ засобів і систем криптографічного захисту інформації регламентується нормативно-правовими актами та нормативними документами з криптографічного захисту інформації.

2.2. Етапи створення КСЗІ

1 етап. Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ

На цьому етапі в загальному випадку виконується:

– аналіз нормативно-правових актів, на підставі яких можуть встановлюватися обмеження доступу до певних видів інформації або заборона такого обмеження, визначається необхідність забезпечення захисту інформації згідно з іншими критеріями;

– визначаються переліки інформації, що підлягає автоматизованій обробці, і здійснюється її класифікація щодо рівня обмеження доступу до неї, вимог щодо забезпечення цілісності та вимог щодо забезпечення доступності відповідно до нормативно-правових актів.

При обстеженні ІТС розглядається як організаційно – технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІТС).

Метою обстеження є опис кожного середовища функціонування ІТС та виявлення в них елементів, які безпосередньо або опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

2 етап. Формування політики безпеки

На цьому етапі здійснюється:

– аналіз ризиків (вивчення моделі загроз та моделі порушника, можливих наслідків від реалізації потенційних загроз);

– визначення вимог до заходів, методів і засобів захисту інформації;

– вибір основних рішень з протидії всім суттєвим загрозам, формування вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, а також регламентують діяльність користувачів всіх категорій;

– документальне оформлення політики безпеки інформації.

Політика безпеки повинна враховувати особливості окремих компонентів КСЗІ та може розроблятися для ІТС в цілому, для окремих складових компонента, для окремої функціональної задачі, для окремої технології обробки інформа-

ції. Політика безпеки оформляється у вигляді окремого документа Плану захисту.

3 етап. Розробка технічного завдання (далі – ТЗ) на створення КСЗІ

Технічне завдання на створення КСЗІ в ІТС є вихідним організаційно-технічним документом, в якому визначаються вимоги щодо захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

Технічне завдання на створення КСЗІ розробляється з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеки інформації на всіх етапах життєвого циклу ІТС.

ТЗ на КСЗІ може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС.

ТЗ на КСЗІ може бути оформлений:

– у вигляді окремого розділу загальної технічної задачі на створення ІТС;

– у вигляді окремого (часткового) ТЗ;

– у вигляді доповнення до загального ТЗ на створення ІТС.

Для інтегрованих ІТС (що складаються з декількох окремих інформаційних чи телекомунікаційних систем, які можуть функціонувати як самостійно, так і взаємодіяти між собою) рекомендується для кожної із складових частин ІТС створювати окремі КСЗІ і оформляти вимоги окремими ТЗ. Можлива розробка одного ТЗ на кілька однотипних складових частин ІТС, вказавши існуючі між ними відмінності або особливості. [6]

4 етап. Розробка і реалізація проекту КСЗІ в ІТС

Проект КСЗІ розробляється на підставі та у відповідності з Технічним завданням на створення ІТС і виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робоча документація.

При розробці проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають можливість забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і засобів захисту інформації.

Виконується розробка спільних рішень, необхідних для реалізації вимог ТЗ на КСЗІ, щодо організаційної структури КСЗІ, структури технічних і програмних засобів, алгоритмів функціонування та умов використання засобів захисту, реалізації визначених функціональним профілем захищеності послуг безпеки інформації.

5 етап. Введення КСЗІ в дію

На цьому етапі повинна бути завершена розробка КСЗІ і затверджені документи, які входять до Плану захисту.

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів) основним положенням та процедурами документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації.

Проводиться атестація впровадженого комплексу технічного захисту інформації від витоку технічними каналами, за результатами якого видається документ: «Акт атестації комплексу технічного захисту інформації».

Здійснюється згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності комплексу засобів захисту інформації від НСД.

Під час інсталяції повинні бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, механізми контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту.

До бази даних захисту вносяться відомості про користувачів ІТС, встановлюються їх повноваження щодо доступу до захищених об'єктах ІТС, їх створення, модифікації, архівування, знищення, експорту / імпорту із системи.

6 етап. Попередні випробування

Метою попередніх випробувань є перевірка працездатності КСЗІ, її відповідності технічним завданням і визначення можливості прийняття КСЗІ в дослідну експлуатацію.

Попередні випробування проводяться у відповідності з програмою і методиками випробувань. Їх організовує замовник ІТС, а проводить – розробник КСЗІ спільно із замовником.

7 етап. Дослідна експлуатація

Під час дослідної експлуатації КСЗІ:

– відпрацьовуються технології захисту оброблюваної інформації, оббіг машинних носіїв інформації, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

– співробітники системи захисту інформації (далі – СЗІ) та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань забезпечення режиму доступу;

– здійснюється доопрацювання програмного забезпечення, додаткове налаштування та конфігурування КЗЗ від НСД;

– здійснюється коригування робочої та експлуатаційної документації.

Дослідна експлуатація ІТС повинна здійснюватися без використання інформації, що становить державну таємницю.

У разі використання в складі КСЗІ комплексу засобів захисту інформації від НСД, який не має експертного висновку про відповідність вимогам НД ТЗІ, необхідно здійснити комплекс робіт з підготовки до проведення оцінки відповідності цього комплексу засобів захисту інформації ви-

могам НД ТЗІ під час проведення державної експертизи КСЗІ.

8 етап. Державна експертиза КСЗІ

Комплексна система захисту інформації, що є власністю держави, або інформації з обмеженим доступом, або іншої інформації, захист якої гарантується державою, повинна мати атестат відповідності вимогам захисту інформації, який видається ДССЗЗІ України за результатами державної експертизи.

Державна експертиза КСЗІ проводиться з метою визначення її відповідності технічному завданню, вимогам нормативно-правових актів і нормативних документів щодо захисту інформації та з метою визначення можливості введення КСЗІ в експлуатацію в складі ІТС.

Державна експертиза КСЗІ є етапом приймальних випробувань ІТС та проводиться у відповідності до Положення про державну експертизу в сфері технічного захисту інформації.

Якщо в ІТС обробляється інформація, яка є власністю держави, або інформація, захист якої гарантується державою, то дозвіл на експлуатацію ІТС дається наказом керівника організації тільки за наявності атестату відповідності КСЗІ.

9 етап. Супровід КСЗІ

На цьому етапі виконуються роботи з організаційного забезпечення функціонування КСЗІ, її планової модернізації та з управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ. [5]

3. РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ

Під політикою безпеки інформації в Системі розуміється набір законів, нормативних документів, вимог, правил, обмежень, інструкцій, рекомендацій, що регламентують порядок обробки інформації і спрямовані на захист інформації від визначених погроз. Політика безпеки розробляється для окремого компонента Системи, послуги захисту і Системи в цілому. Політика безпеки інформації в Системі є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи і положення.[4]

Виходячи з міжнародного досвіду та вимог міжнародних стандартів в області інформаційної безпеки розрізняють три типи ПБ (рис. 2).

Програмна ПБ – є політикою вищої ланки управління в організації. Об'єктом є організація в цілому, за розробку і здійснення програмної політики несе відповідальність керівництво організації. Програмна політика визначає стратегічні напрямки забезпечення інформаційної безпеки (далі – ІБ).

Системно – орієнтована політика – структура, склад, вимоги до етапу документування, які визначені вітчизняними нормативними документами.

Проблемно – орієнтована політика. Об'єктом такої політики є окрема проблема чи завдання в області забезпечення ІБ. Існує ряд областей діяльності організації, для яких необхідно розробити проблемно – орієнтовану політику.

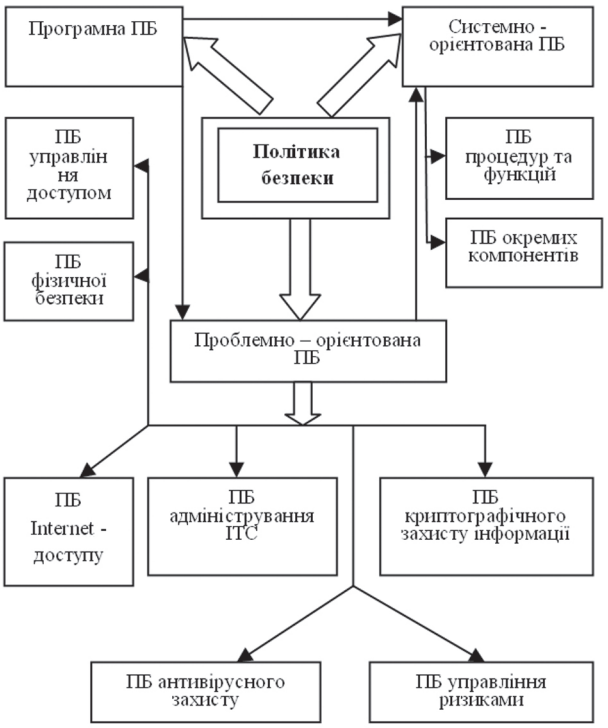


Рис. 2. Типи політики безпеки

Зміст політики безпеки Системи визначається технологією обробки інформації, моделями порушників і погроз, особливостями обчислювальної системи, фізичного середовища й інших факторів. Унаслідок цього, якщо в якій-небудь Системі реалізуються різні технології обробки інформації, то і політика безпеки в такій Системі буде складатися з декількох істотно відмінних частин, кожна з яких буде відповідати конкретної технології обробки інформації. Як складові частини загальної політики безпеки Системи можуть розроблятися політики забезпечення конфіденційності, цілісності, спостережності і доступності оброблюваної інформації, а також правила розмежування доступу (ПРД), що регламентують правила доступу користувачів і процесів до ресурсів Системи.

Політика безпеки повинна передбачати комплексне використання правових і морально-етичних норм, організаційних (адміністративних) мір, фізичних, технічних (апаратних і програмних) способів і засобів захисту інформації, а також визначати правила і порядок їхнього застосування в Системі. Політика безпеки повинна базуватися на принципах системності, комплексності, безперервності захисту, достатності механізмів і заходів захисту і їхньої адекватності погрозам, гнучкості керування системою захисту, простоти і зручності її використання, відкритості алгоритмів і механізмів захисту, якщо інше не передбачене окремо.[3]

Політика безпеки Системи повинна доказово давати гарантії того, що:

– у Системі (у кожній окремій складовій частині, у кожній функціональній задачі) забезпечується адекватність рівня захисту інформації рівню її критичності;

– реалізація заходів захисту інформації є рентабельної;

– у будь-якім середовищі функціонування Системи забезпечується оцінка і перевірка захищеності інформації;

– забезпечується персоніфікація положень політики безпеки (щодо суб'єктів Системи), звітність (реєстрація, аудит) для всіх критичних з погляду безпеки ресурсів, до яких здійснюється доступ;

– персонал і користувачі забезпечені досить повним комплектом документації щодо порядку забезпечення захисту інформації;

– усі критичні з погляду безпеки інформації технології (функції) Системи мають відповідні плани забезпечення безупинної роботи і її поновлення у випадку виникнення непередбачених ситуацій.

Методологія розробки політики безпеки містить у собі наступні роботи:

– розробка концепції безпеки інформації в Системі;

– аналіз ризиків;

– визначення вимог до методів і засобів захисту;

– вибір основних рішень по забезпеченню безпеки інформації;

– організація виконаних робіт і забезпечення безупинного функціонування Системи;

– документальне оформлення політики безпеки.

У загальному випадку документ «Політика безпеки Системи» повинний містити в собі опис:

1. Об’єктів (елементів ресурсів) Системи;
2. Основних погроз інформації;
3. Вимог по захисту від погроз;
4. Принципів керування доступом користувачів до інформації;
5. Правил розмежування інформаційних потоків;
6. Правил маркірування носіїв інформації;
7. Основних атрибутів доступу користувачів, процесів і пасивних об’єктів;
8. Правил розмежування доступу користувачів і процесів до пасивних об’єктів;
9. Правил адміністрування КСЗІ і реєстрації дій користувачів. [7]

У розділі «Опис об’єктів (елементів ресурсів) Системи» на основі інвентаризації (ідентифікації) усіх компонентів Системи, що беруть участь у технологічному процесі обробки інформації, приводиться опис критичних з погляду безпеки активних і пасивних компонентів Системи.

Інвентаризації (ідентифікації) підлягають:

– організаційно-топологічна структура Системи, для якої створюється КСЗІ;

– склад і призначення функціональних підсистем Системи;

– склад служб і протоколів, що реалізують інформаційний обмін між елементами (компонентами) Системи;

– об'єкти захисту (види і категорії оброблюваної інформації, апаратно-програмні й інформаційні ресурси на відповідних рівнях ієрархічної структури Системи);

– персонал і користувачі Системи.

При описі компонентів Системи рекомендується скласти структурну схему інформаційних потоків між основними компонентами Системи, а також описати (чи формально неформально) технологію обробки інформації. При виборі й аналізі об'єктів Системи важливим моментом є ступінь деталізації розглянутих об'єктів. Так, для Системи 1-го класу (окрема ПЕОМ) припустимо розглядати всю інфраструктуру, тоді як для Системи 3-го класу (глобальна мережа) всеосяжна оцінка може зажадати неприйнятних витрат часу і сил. У цьому випадку рекомендується зосередитися на описі найбільш важливих компонентів Системи.

У розділі «Опис основних погроз інформації» на основі аналізу ризиків приводиться перелік і класифікація можливих видів погроз безпеки інформації в Системі. Під погрозою безпеки розуміються які-небудь чи обставини дії, що можуть бути причиною порушення політики безпеки інформації чи нанесення збитку Системі. Збиток полягає в порушенні якості інформації користувачів (у семантичному і прагматичному змісті) шляхом її знищення, чи зміни несанкціонованого одержання, або в знищенні, чи зміні несанкціонованому використанні ресурсів Системи. У залежності від класу Системи аналіз погроз необхідно здійснювати на рівні окремих апаратних, апаратно-програмних і програмних засобів, окремої локальної обчислювальної мережі, глобальної мережі. Аналіз ризиків передбачає розробку моделі погроз для інформації і моделі порушника, установлення відповідності моделі погроз і об'єктів захисту, оцінку можливості реалізації погрози (оцінка ризику), кількісну або якісну оцінку величини можливого збитку внаслідок реалізації погроз конфіденційності, цілісності, спостережності чи доступності інформації або втрати керованості Системи. Для розробки моделі погроз необхідно сформувати перелік основних погроз і описати можливі способи їхнього здійснення на основі аналізу об'єктів Системи, характеристик обчислювальної системи, фізичного середовища, персоналу, особливостей функціонування Системи.

У розділі «Вимоги по захисту від погроз» приводяться основні задачі і мети захисту інформації, об'єкти захисту, обраний варіант побудови КСЗІ Системи. З урахуванням класу Системи для кожного компонента і Системи в цілому перелічуються функціональні послуги безпеки і вимоги до рівнів реалізації кожної з них, рівень гарантій реалізації послуг. Для кожного компонента і Системи в цілому визначаються загальні підходи і вимоги по захисту інформації від витоку технічними

каналами. На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоку технічними каналами. При необхідності визначаються компоненти Системи, для яких доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки Системи. Вихідними даними для розробки вимог по захисту від погроз є задачі і функції Системи, результати аналізу середовища функціонування Системи, модель погроз, модель порушників, результати аналізу ризиків.

У розділі «Опис принципів керування доступом користувачів до інформації» приводяться обраний метод керування доступом (довірче і адміністративне керування), вимоги до забезпечення безперервності захисту, до набору атрибутів доступу і правилам їхнього використання (присвоєння, застосування, зміна, скасування), до реєстрації дій користувачів при використанні ресурсів Системи, а також інших подій, що впливають на дотримання реалізованої в Системі політики безпеки.

У розділі «Опис правил розмежування інформаційних потоків» приводиться перелік інформаційних потоків, що циркулюють між компонентами Системи. У залежності від класу Системи структурна схема інформаційних потоків між основними компонентами Системи може включати:

– внутрішні потоки обміну між активними і пасивними об'єктами усередині однієї ПЕОМ;

– локальні потоки обміну між робочими станціями і серверами усередині однієї ЛОМ (домена);

– міжмережеві потоки обміну між ЛОМ (доменами), що входять до складу однієї Системи;

– потоки обміну інформацією з вилученими взаємодіючими об'єктами, що не входять до складу Системи.

Правила розмежування інформаційних потоків формулюються на основі аналізу області (границі) існування, спрямованості (вхідні чи вихідні), джерел і приймачів, функціонального призначення потоків, вимог по забезпеченню конфіденційності, цілісності, спостережності і доступності. Правила повинні визначати, де і на яких рівнях взаємодії систем повинне здійснюватися розмежування інформаційних потоків і з використанням яких атрибутів і механізмів (ідентифікаторів безпеки, мережних портів, ключів аутентифікації, ключів напрямків і мережних ключів шифрування). Правила повинні також визначати умови й обмеження по ініціюванню і завершенню процесів інформаційного обміну, наприклад, у виді асоціації безпеки.

У розділі «Опис правил маркірування носіїв інформації» приводяться правила, що регламентують порядок обліку, збереження, копіювання, використання і знищення носіїв інформації. Правила формулюються на основі вивчення форм існування критичної інформації на всіх етапах життєвого циклу Системи, середовища функціонування Системи, моделі погроз для інформації і моделі порушників, результатів аналізу ризиків, вимог по забезпеченню конфіденційності, цілісності, спостережності і доступності інформації.

У розділі «Опис основних атрибутів доступу користувачів, процесів і пасивних об'єктів» приводяться склад атрибутів доступу (ідентифікаційні імена, індивідуальні і групові ідентифікатори безпеки, паролі, мітки і /чи маркери доступу, списки контролю доступу), вимоги до характеристик атрибутів доступу (приналежність, унікальність, розмірність, терміни дії) і правила роботи з ними (присвоєння, використання, модифікація, скасування).

У розділі «Опис правил розмежування доступу користувачів і процесів до пасивних об'єктів» міститься набір правил визначальних склад обличчя, яким дозволений доступ до ресурсів Системи, порядок правильного використання ресурсів Системи, статус, права і привілеї адміністратора безпеки Системи, статус, права і привілеї користувачів Системи.

У розділі «Опис правил адміністрування КСЗІ і реєстрації дій користувачів» приводиться порядок адміністрування облікових записів користувачів, профілів користувачів, груп користувачів, загальних ресурсів і аудита.

4. РОЗРОБКА ТЕХНІЧНОГО ЗАВДАННЯ

Вимоги до порядку розробки, складу й змісту ТЗ на створення КСЗІ в АС, призначеної для обробки, збереження і передачі інформації досить повно встановлює нормативні документи, згідно з якими ТЗ на КСЗІ в загальному випадку повинно містити такі основні розділи:

– загальні відомості;

– мета і призначення комплексної системи захисту інформації;

– загальна характеристика автоматизованої системи та умов її функціонування;

– вимоги до комплексної системи захисту інформації;

– вимоги до складу проектної та експлуатаційної документації;

– етапи виконання робіт;

– порядок внесення змін і доповнень до ТЗ;

– порядок проведення випробувань комплексної системи захисту інформації. [3]

Розробка ТЗ на комплексну систему захисту інформації являє собою самостійний, досить складний і трудомісткий процес, що включає роботи, основний склад яких виконується на попередньому етапі створення КСЗІ.

Технічне завдання на створення КСЗІ в АС поряд із законодавчими актами, стандартами та нормативними документами ДССЗЗІ України в області захисту інформації є обов'язковим основоположним організаційно-технічним документом при виконанні робіт із забезпечення захисту

інформації в системі, а також під час проведення експертизи АС на відповідність вимогам захищеності інформації. В організаційному аспекті, головне завдання ТЗ на КСЗІ – забезпечити нормативно-технічну базу взаємодії Замовника (власника або користувача АС) КСЗІ, Розробника КСЗІ та експертної організації у процесі розробки, виробництва (впровадження), випробувань, оцінки безпеки інформації та експлуатації КСЗІ.

Для Замовника КСЗІ технічне завдання є документом, що дозволяє на підставі результатів проведеного аналізу ризиків та обраної політики безпеки сформулювати запити до захисту АС у вигляді стандартизованих вимог.

Для Розробника технічне завдання на КСЗІ є керівним документом, що дозволяє на підставі результатів проведеного аналізу запитів Замовника КСЗІ:

– визначити завдання захисту і набір вимог безпеки (функціональних вимог, вимог гарантій та вимог до середовища експлуатації), яким повинна задовольняти, розробляється КСЗІ;

– довести, що вимоги безпеки реалізовані з заданим рівнем гарантій;

– визначити умови, які необхідно виконати для успішного виконання оцінки безпеки інформації готового продукту інформаційної технології.

Для експертної організації ТЗ на КСЗІ є документом, що визначає основні критерії відповідності КСЗІ вимогам Замовника і загрозам, що діють у середовищі експлуатації.

Рівень складності розробки, зміст, вимоги і складові частини ТЗ на КСЗІ визначаються:

– класом, що захищається АС (одномашинний однокористувацький комплекс, локальний багатомашинний багатокористувацький або глобальна мережа);

– організаційно-топологічної структурою;

– способами організації взаємодії між компонентами АС;

– обсягом завдань захисту інформації, сформульованих Замовником (користувачем) АС;

– адекватністю моделі загроз реальних умов експлуатації АС.

Істотну роль відіграють початкові умови розробки ТЗ на КСЗІ – створення захищеного АС з "нуля" або модернізація КСЗІ для існуючої (функціонуючої) АС.

За будь-яких початкових умовах розробка ТЗ на КСЗІ для АС класу 1 (одномашинний однокористувацький комплекс) особливих проблем не викликає внаслідок прозорість всієї інформаційної інфраструктури.

У разі створення захищеної АС з "нуля" при розробці ТЗ на КСЗІ для АС класу 2 (локальний багатомашинний багатокористувацький комплекс) і особливо класу 3 (глобальна мережа) внаслідок того, що ТЗ на КСЗІ і основне ТЗ на АС розробляються паралельно (одночасно) виникає ряд факторів, що впливають на складність розробки, зміст, вимоги і складові частини ТЗ на КСЗІ.

Перший фактор полягає в тому, що загально технічні вимоги (ЗТВ) до архітектури АС (функціональної та організаційно-топологічної структурі, інформаційного, програмного і технічного забезпечення) і розробка вимог до КСЗІ формуються одночасно, внаслідок чого створюється дефіцит часу для розробника ТЗ на КСЗІ. При цьому ЗТВ є вихідними даними для проведення аналізу ризиків, розробки політики безпеки і підрозділу «Загальна характеристика автоматизованої системи та умови її функціонування». Для виключення випадків порушення встановлених строків подання ТЗ Замовнику необхідно при складанні графіка розробки ТЗ враховувати цю особливість і жорстко регламентувати роботу виконавців.

Другий фактор полягає в тому, що класифікація і опис ресурсів АС, розробка інформаційної моделі, аналіз ризиків та розробка політики безпеки проводяться в умовах апріорної невизначеності щодо кінцевих загальних характеристик АС та умов її функціонування тому остаточна архітектура, технічні характеристики та особливості функціонування захищається АС будуть сформовані тільки на стадії ескізно-технічного проектування. Тому за результатами етапів виконаних робіт зі створення захищеної АС технічне завдання на КСЗІ повинно коректуватися з оформленням додатків в тому ж порядку, що й основний документ.

Третій чинник пов'язаний з процедурами аналізу ризиків і розробкою політики безпеки і полягає у виборі та визначення ступеня деталізації розгляду об'єктів інформаційної інфраструктури. Дана обставина обумовлена тим, що всеохоплююча оцінка може зажадати неприйнятних витрат часу і сил. У цьому випадку доцільно зупинитися на деякій рівні деталізації, визначивши найбільш важливі об'єкти, ризики для яких найбільш великі, і погоджуючись з наближеністю підсумкової оцінки.

Для створюваної з «нуля» АС класу 3, складність розробки, зміст, вимоги і складові частини розділів «Мета і призначення комплексної системи захисту інформації» та «Вимоги до комплексної системи захисту інформації» ТЗ на КСЗІ АС визначаються організаційно-топологічною структурою, способами організації взаємодії між компонентами АС, складністю вибору та обґрунтування функціонального профілю захищеності від НСД і вимог до захищеності інформації від витоку технічними каналами.

Дана обставина обумовлена тим, що АС класу 3 (глобальна мережа), як правило, являє собою сукупність складових частин, що є АС класу 2 (локальні багатомашинних багатокористувацькі комплекси) і АС класу 1 (одномашинний однокористувацький комплекси).

АС класу 2 і АС класу 1 можуть об'єднуватися допомогою відомчої виділеної середовища пере-

дачі або через загальнодоступні канали зв'язку (приклад Internet, канали телефонної мережі). В останньому випадку використання служб і механізмів захисту інформації дозволяє будувати віртуальні захищені мережі (VPN).

Кожна складова частина має свою архітектуру, зовнішнє середовище, обслуговуючий персонал та інформаційні технології. Внаслідок цього, в залежності від сформульованих Замовником (користувачем) АС завдань захисту, політики безпеки та умов експлуатації, кожна із складових частин АС класу 3 може відрізнятися від іншої підкласом, складом функціональних послуг безпеки, рівнем гарантій та вимог до захищеності інформації від витоку технічними каналами.

З позицій системного підходу до складу функціональних послуг безпеки окремих складових частин КСЗІ АС класу 3 можуть включатися функції безпеки не притаманні цієї складової частини і забезпечують прояв якого-небудь системного властивості КСЗІ АС класу 3.

Вибір і обґрунтування функціонального профілю захищеності та рівня гарантій окремої складової частини КСЗІ АС класу 3 повинен здійснюватися не тільки на основі її підкласу, але і з урахуванням вимог до загальносистемних послуг безпеки.

Вибір і обґрунтування функціонального профілю захищеності АС класу 3 здійснюється шляхом інтеграції функціонального профілів складових частин з виділенням функціональних послуг безпеки і рівнів гарантій, притаманних КСЗІ.

Зміст розділу «Вимоги до комплексної системи захисту інформації» ТЗ на КСЗІ АС та вимоги до функціональних послуг безпеки істотно залежать від способів утворення захищених віртуальних каналів і вимог замовника за ступенем захищеності інформації, що циркулює у відкритих каналах зв'язку. Дана обставина робить істотний вплив на:

– вибір вимог до функцій і рівнями гарантій криптографічного захисту інформації;

– формування принципів і варіантів організації захищених віртуальних каналів;

– визначення ініціаторів і термінаторів тунелю;

– вибір протоколів тунелювання, методів автентифікації і шифрування.

Для створюваної з «нуля» АС класу 3 зміст розділу «Вимоги до комплексної системи захисту інформації» ТЗ на КСЗІ може включати в якості підрозділів вимоги до функціональних послуг безпеки та рівнями гарантій окремих складових частин (АС першого та другого класів).

Доцільність введення окремих підрозділів для складових частин АС визначається в кожному конкретному випадку залежно від ступеня «неспівпадання» політик безпеки та умов експлуатації, підкласів, складів функціональних послуг безпеки, рівнів гарантій та вимог до захищеності інформації від витоку технічними каналами.

Для розробки ТЗ на КСЗІ АС класу 3 (глобальна мережа) в додаток до функціонального профілю захищеності, обов'язковими вихідними даними повинні бути завдання захисту, політика і концепція безпеки АС, сформовані Замовником (користувачем) АС.

Під завданнями захисту розуміється потреба замовника АС (споживача інформаційної технології) в протистоянні безлічі загроз безпеки або в необхідності реалізації політики безпеки за певних умов експлуатації АС.

Прикладами завдань захисту інформації можуть бути:

– забезпечення певних політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення й експлуатації АС;

– своєчасне виявлення і знешкодження загроз для ресурсів АС, причин та умов, які можуть призвести до порушення її функціонування та розвитку;

– ефективне блокування (попередження) загроз для ресурсів АС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;

– управління засобами захисту інформації, керування доступом користувачів до ресурсів АС, контроль за їх роботою з боку персоналу КСЗІ, оперативне сповіщення про спроби НСД до ресурсів АС;

– реєстрація, збір, збереження, обробка даних про всі події в системі, які мають відношення до безпеки інформації.

При виборі і обґрунтуванні задач захисту для кожної складової частини АС третього класу має бути показано, що пропонований склад завдань відповідає параметрам середовища експлуатації, а їх рішення дозволить ефективно протистояти певним загрозам безпеки і реалізувати політику безпеки, визначену для даної складової частини і АС.

Розробка політики і концепції безпеки в АС будь-якого класу повинна передувати розробці ТЗ на створення КСЗІ.

При виборі і обґрунтуванні функціонального профілю захищеності для кожної складової частини АС класу 3 необхідно забезпечити такий рівень деталізації вимог, який дозволяє показати їх відповідність завданням захисту даної АС. При виборі і обґрунтуванні вимог до функціональних послуг безпеки повинні бути дотримані наступні умови:

– сукупність цілей функціональних послуг безпеки повинні відповідати встановленим завданням захисту;

– вимоги безпеки повинні бути узгодженими, тобто не суперечити один одному, а навпаки – взаємно підсилювати.

При розробці ТЗ на модернізацію КСЗІ для існуючої (функціонуючої) АС повинні бути прийняті до уваги причини проведення модернізації.

Необхідність модернізації КСЗІ існуючої АС будь-якого класу може бути обумовлена наступним:

– подальшим розвитком і вдосконаленням існуючої АС;

– зміною Замовником (користувачем) АС завдань захисту інформації;

– появою нових загроз.

У першому випадку особливості розробки ТЗ на модернізацію КСЗІ існуючої АС будь-якого класу аналогічні розробки ТЗ на КСЗІ для АС створюваної з «нуля».

У другому і третьому випадках основна особливість розробки ТЗ на модернізацію КСЗІ існуючої АС будь-якого класу полягає в тому, що в загальному випадку впровадження комплексів засобів захисту (КЗЗ) потребують внести істотні зміни в загальносистемні і технічні характеристики існуючої АС, що пов'язано з фінансовими витратами в додаток до витрат на створення КСЗІ. Тому при формуванні вимог безпеки (функціональних вимог, вимог гарантій та вимог до середовища експлуатації), що забезпечують реалізацію задач захисту, необхідно визначити по можливості повно можливі структурні і технічні зміни в архітектурі існуючої АС, викликані необхідністю досягнення необхідного рівня захищеності, та можливість їх реалізації Замовником [8].

КСЗІ в АС будь-якого класу реалізується комплексним застосуванням методів технічного та криптографічного захисту інформації в автоматизованій системі. Обов'язковим є включення у склад вимог до послуг безпеки (конфіденційність, цілісність, доступність і неспростовність) та рівнями гарантій вимог до функцій і рівнями гарантій криптографічного захисту інформації, наприклад таких, як:

а) управління ключами:

– генерація ключів заданого розміру за певними алгоритмами відповідно до спеціальних стандартами;

– розподіл ключів способами, визначеними в спеціальних стандартах;

– здійснення доступу до ключів з використанням методів, визначених у спеціальних стандартах;

– знищення ключів з використанням методів, визначених у спеціальних стандартах;

б) криптографічні засоби:

– виконання криптографічних операцій з використанням ключів заданого розміру і певних алгоритмів у відповідності зі спеціальними стандартами.

Вимоги до функцій і рівнями гарантій криптографічного захисту інформації в обов'язковому порядку повинні включатися до опису функціонального профілю захищеності, який повинен бути реалізований в АС.

ВИСНОВКИ

В даній статті особлива увага приділяється передпроектним роботам КСЗІ, а саме: розробці політики безпеки та технічному завданню.

На етапі розробки політики безпеки розробник КСЗІ проводить детальне вивчення об'єкта, на якому створюється КСЗІ, уточнює моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками, які виконані на попередніх етапах, а також виконує у разі необхідності додаткові науково-дослідні роботи (НДР), пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, оформлює і затверджує звіти з НДР, що виконувалися.

Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації.

Політика безпеки залежить від:

– конкретної технології обробки інформації;

– використаних технічних і програмних засобів;

– розташування організації.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.4-001 «Типове положення про службу захисту інформації в інформаційно-телекомунікаційних системах».[7]

В технічному завданні вказуються призначення об'єкта, область його застосування, стадії розробки конструкторської (проектної, технологічної, програмної) документації, її склад, терміни виконання, а також особливі вимоги, зумовлені специфікою самого об'єкту або умовами його експлуатації. Як правило, ТЗ складають на основі аналізу результатів попередніх досліджень, розрахунків і моделювання.

Як інструмент комунікації спілкування замовник-виконавець, технічне завдання дозволяє: обом сторонам:

– представити готовий продукт;

– виконати поетапно перевірку готового продукту (приймальне тестування – проведення випробувань);

– зменшити число помилок, пов'язаних зі зміною вимог в результаті їх неповноти або хибності (на всіх стадіях і етапах створення, за винятком випробувань).

Замовнику:

– усвідомити, що саме йому потрібно;

– вимагати від виконавця відповідності продукту всім умовами, що вказані в ТЗ.

Виконавцю:

– зрозуміти суть завдання, показати замовнику «технічний вигляд» майбутнього виробу, програмного виробу або автоматизованої системи;

– спланувати виконання проекту і працювати за наміченим планом;

– відмовитися від виконання робіт, не зазначених у ТЗ.

Література.

[1] Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 року, № 2594-IV, К., 2005.

[2] Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-2005.

[3] *Марущак А.І.* Правові основи захисту інформації з обмеженим доступом: курс лекцій. – К.: КНТ, 2007.-208 с.

[4] *Бондаренко М.Ф., Черних С.П., Горбенко І.Д., Замула А.А., Ткач А.А.* Методические основы концепции и политики безопасности информационных технологий. Радиотехника. 2001. Вып.119.с.5-17.

[5] Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. НД ТЗІ 1.1-005-07.

[6] Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. НД ТЗІ 3.1-001-07.

[7] Типове положення про службу захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 1.4-001.

[8] Методологічні вказівки щодо розробки ТЗ на створення КСЗІ в АС. НД ТЗІ 3.7-001-99.

Надійшла до редколегії 30.06.2010.

Землянко Юлія Валеріївна, асистент кафедри інформаційних технологій ХДУХТ. Область наукових інтересів: наукове обґрунтування напрямків активізації дослідження. Використання у навчальному процесі ігрових методик, відео- та медіа технологій.

Замула Олександр Андрійович, професор кафедри БІТ ХНУРЕ, канд. техн. наук, доцент. Область наукових інтересів: технології захисту інформації в інформаційно-телекомунікаційних системах.

Ткач Александр Александрович, заместитель главного конструктора ЗАО «Институт информационных технологий». Область научных интересов: безопасность информационных технологий, методология создания и оценки эффективности комплексных систем защиты информации в информационных и информационно-телекоммуникационных системах.

Литвинова Наталья Ивановна, студентка кафедры БИТ ХНУРЭ. Область научных интересов: вопросы построения комплексных систем защиты информации в информационно-телекоммуникационных системах.

Пересичанская Ярослава Андреевна, студентка кафедры БИТ ХНУРЭ. Область научных интересов: вопросы построения комплексных систем защиты информации в информационно-телекоммуникационных системах.

УДК 004.056.5

Принципы и порядок разработки комплексных систем защиты информации в информационно-телекоммуникационных системах / Ю.В. Землянко, А.А Замула, А.А. Ткач, Н.И. Литвинова, Я.А. Пересечанская // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 460–469.

Рассматривается порядок осуществления мер и применения средств защиты при создании комплексных систем защиты информации в современных информационно – телекоммуникационных системах.

Ключевые слова: комплексные системы защиты информации, информационно-телекоммуникационные системы.

Ил.02. Библиогр.: 08 назв.

UDC 004.056.5

Principles and order of developing complex information security systems in information and telecommunication systems / U.V. Zemlyanko, A.A. Zamula, A.A. Tkach, N.I. Litvinova, Y.A. Peresechanskaya // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 460-469.

A procedure for implementing measures and using means to create complex systems of information protection in modern information and telecommunication systems is considered.

Key words: complex systems of information protection, information and telecommunications systems.

Fig. 02. Ref.: 08 items.

УДК 621.396

ВСТРАИВАНИЕ ИНФОРМАЦИОННЫХ ДАННЫХ В НЕПОДВИЖНЫЕ ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ПРЯМОГО РАСШИРЕНИЯ СПЕКТРА

А.А. КУЗНЕЦОВ, А.М. БОТНОВ, П.А. ЛАПТИЙ

Исследуются стеганографические методы встраивания данных в неподвижные изображения для скрытной передачи информации. Рассматривается метод стеганографической защиты, основанный на использовании прямого расширения спектра дискретных сигналов, исследуется его эффективность с точки зрения обеспечиваемой стойкости, пропускной способности и величины вносимых искажений в контейнер-изображение.

Ключевые слова: метод расширения спектра, дискретный сигнал, корреляционный прием, стеганографическая защита информации.

1. ПОСТАНОВКА ПРОБЛЕМЫ В ОБЩЕМ ВИДЕ И АНАЛИЗ ЛИТЕРАТУРЫ

Важным направлением в развитии современных средств защиты информации являются стеганографические системы, которые обеспечивают сокрытие в тайне от противника не только информационного содержания передаваемых данных, но и самого факта передачи сообщений [1, 2]. Наиболее перспективными являются стеганографические методы, построение которых базируется на развитом математическом аппарате теории дискретных сигналов и помехозащищенной передачи данных [3–7].

Целью данной статьи является исследование стеганографического метода встраивания данных в неподвижные изображения [2], основанного на использовании прямого расширения спектра дискретных сигналов, оценка его эффективности с точки зрения обеспечиваемой стойкости, пропускной способности и величины вносимых искажений в контейнер-изображение.

2. ПРЯМОЕ РАСШИРЕНИЕ СПЕКТРА В ТЕОРИИ СВЯЗИ

Для построения современных помехозащищенных систем цифровой связи используются методы теории дискретных сигналов, корреляционного и спектрального анализа [3–7]. С точки зрения эффективного использования частотно-временных и энергетических ресурсов каналов связи наиболее перспективными считаются широкополосные системы с шумоподобными дискретными сигналами и прямым расширением спектра [3, 4].

Под дискретным сигналом будем понимать информационный сигнал, который представляется в виде отдельных значений, взятых по времени. Далее мы будем рассматривать дискретный сигнал как двоичную псевдослучайную последовательность (ПСП) $\Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right)$ длины n из множества $\Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\}$ мощности $|\Phi| = M$ [6].

Элементы двоичной ПСП принимают одно из значений:

$$\varphi_{i_z} = \begin{cases} +1 \\ -1 \end{cases}, \; z = 0, ..., n-1 . \qquad (1)$$

Для построения помехозащищенной широкополосной связи используют понятие корреляции дискретных сигналов - статистической взаимосвязи двух или нескольких ПСП. Математической мерой коррелированности (похожести) двух дискретных сигналов $\Phi_i, \Phi_j \in \Phi$ служит коэффициент корреляции $\rho(\Phi_i, \Phi_j)$ [3, 4]:

$$\rho\left(\Phi_i, \Phi_j\right) = \frac{1}{n} \sum_{z=0}^{n-1} \Phi_{iz} \Phi_{j_z} . \qquad (2)$$

Два сигнала Φ_i, Φ_j называют ортогональными, если коэффициент корреляции $\rho(\Phi_i, \Phi_j) = 0$. Если $\rho(\Phi_i, \Phi_j) \approx 0$ будем называть сигналы Φ_i и Φ_j квазиортогональными [5, 7].

В работах [3 – 5, 7] исследованы различные подходы к построению дискретных сигналов с улучшенными ансамблевыми и корреляционными свойствами: производные ортогональные системы сигналов (ПОСС); нелинейные производные кодовые последовательности (НПКП); полные кодовые кольца (ПКК); последовательности Голда. В табл. 1 в качестве примера приведены результаты исследований ансамблевых и корреляционных свойств производных систем сигналов [7].

Таблица 1

Ансамблевые и корреляционные свойства дискретных сигналов

n	M	ρ
64	$\approx 10^3$	$2{,}1/\sqrt{n}$
128	$\approx 10^4$	$2{,}5/\sqrt{n}$
256	$\approx 10^6$	$2{,}9/\sqrt{n}$
512	$\approx 10^7$	$3{,}2/\sqrt{n}$
1024	$\approx 10^8$	$3{,}5/\sqrt{n}$
2048	$\approx 10^9$	$3{,}8/\sqrt{n}$
4096	$\approx 10^{10}$	$3{,}9/\sqrt{n}$

Как следует из приведенных в табл. 1 данных, применение производных ортогональных диск-

ретных сигналов позволяет при сохранении низкой коррелированности дискретных последовательностей ($\rho(\Phi_i,\Phi_j)\approx 0$) существенно повысить мощность M ансамблей дискретных сигналов, с ростом длины последовательностей эта тенденция усиливается.

В современной теории цифровой связи большие ансамбли слабокоррелированных дискретных сигналов используются для построения широкополосных помехозащищенных систем передачи данных. Передаваемые сообщения в таких каналах приобретают вид шумоподобных последовательностей, а за счет большой мощности ансамблей дискретных сигналов и прямого расширения частотного спектра обеспечивается высокая имитостойкость, помехозащищенность и скрытность цифровых каналов связи [3 – 5].

Для передачи данных в широкополосной системе связи информационный сигнал $x(t)=\begin{cases}+1\\-1\end{cases}$ модулируется посредством его умножения на расширяющий кодовый сигнал $g(t)=\Phi_i\in\Phi$ – псевдослучайную последовательность из рассмотренных выше ансамблей дискретных сигналов. Поскольку кодовый сигнал по своим статистическим свойствам подобен шуму, то полученный расширенный сигнал

$$y'(t)=y(t)+e(t) \qquad (3)$$

слабо отличим от шумов в канале связи, что и позволяет осуществить скрытую передачу.

При приеме в демодуляторе полученный сигнал $y'(t)=y(t)+e(t)$ как смесь переданной последовательности $y(t)$ и произошедших в канале связи ошибок $e(t)$ умножается на синхронизированную копию расширяющего сигнала $g(t)$. Другими словами, на приемной стороне осуществляется вычисление коэффициента корреляции (2), значение которого определяет правило принятия решения:

$$\rho\left(y'(t),g(t)\right)=\frac{1}{n}\sum_{z=0}^{n-1}x(t)\Phi_{i_z}\Phi_{i_z}+\frac{1}{n}\sum_{z=0}^{n-1}e(t)\Phi_{i_z}.$$

Учитывая псевдослучайность Φ_i, используемых в качестве $g(t)$, вторым слагаемым в правой части равенства можно пренебречь (количество «+1» примерно равно количеству «-1»), т.е.

$$\begin{aligned}\rho\left(y'(t),g(t)\right)&\approx\rho\left(y(t),g(t)\right)=\\&=x(t)\frac{1}{n}\sum_{z=0}^{n-1}\left(\Phi_{i_z}\right)^2=x(t),\end{aligned} \qquad (4)$$

т.е. значение информационного сигнала на приемной стороне определяется по выражению

$$x(t)=\begin{cases}+1,\text{ при }\rho\left(y'(t),g(t)\right)\approx+1;\\-1,\text{ при }\rho\left(y'(t),g(t)\right)\approx-1;\end{cases} \qquad (5)$$

где знак «≈» предполагает наличие ошибок $e(t)$, вызванных естественными или преднамеренными помехами в канале связи.

Структурная схема приема-передачи информации с использованием прямого расширения спектра приведена на рис. 1.

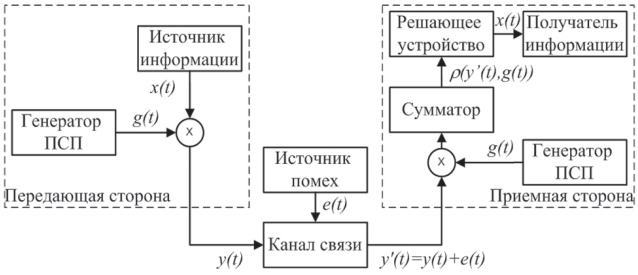


Рис. 1. Структурная схема передачи приема-передачи информации с использованием прямого расширения спектра

Предположим, что временная длительность немодулированного сигнала $x(t)$ равна T, а его частота соответственно равна $F\left(x(t)\right)=\frac{1}{T}$. Передача модулированного сигнала $y(t)$ при той же временной длительности T приведет к расширению частотного спектра передаваемого сигнала, пропорционально числу элементов псевдослучайной последовательности, т.е. пропорционально длине n: $F\left(y(t)\right)=n\frac{1}{T}=nF\left(x(t)\right)$. Тем не менее, использование прямого расширения спектра передаваемого сигнала обеспечивает одновременную передачу многих других информационных сигналов в той же полосе частот. Это следует из взаимной ортогональности (квазиортогональности) применяемых ансамблей дискретных сигналов. Действительно, если на приемной стороне принята аддитивная смесь $\sum_l y_l(t)$ нескольких модулированных сигналов, тогда вычисление коэффициента корреляции даст следующее:

$$\rho\left(\sum_l y_l(t),g(t)\right)=\frac{1}{n}\sum_l\sum_{z=0}^{n-1}x_l(t)\Phi_{l_z}\Phi_{i_z}. \qquad (6)$$

Но все последовательности из множества Φ имеют низкое значение взаимной корреляции, т.е. при $l\neq i$ имеем $\rho(\Phi_l,\Phi_i)=0$ (для ортогональных сигналов имеем равенство $\rho(\Phi_l,\Phi_i)=0$. Следовательно, всеми слагаемыми при $l\neq i$ в правой части равенства (6) можно пренебречь. Отсюда, при наличии в аддитивной смеси $\sum_l y_l(t)$ дискретного сигнала $\Phi_{l=i}$ имеем выражение (4) и соответствующее правило принятия решения (5).

Метод прямого расширения спектра нашел практическое использование в системах цифровой связи с кодовым разделением каналов (CDMA), где для каждого абонента информационного обмена используются уникальные расширяющие кодовые сигналы из ансамбля ортогональных (квазиортогональных) последовательностей. Т.е. для различения кодовых сигналов и разделения соответствующих абонентских каналов используемые ПСП должны быть слабо коррелированны

друг с другом, в идеальном случае – ортогональными.

Так, например, в стандарте CDMA IS-95 для кодового разделения каналов используются ортогональные дискретные сигналы Уолша-Адамара [4]. Они образуются из строк матрицы Адамара H_i, формируемой по рекуррентному правилу:

$$H_i = \begin{bmatrix} H_{i-1} & H_{i-1} \\ H_{i-1} & -H_{i-1} \end{bmatrix}, \; H_0 = [1]. \qquad (7)$$

Многократное повторение правила (7) позволяет сформировать матрицу Адамара любого размера, кратного четырем. Строки сформированных матриц взаимноортогональны, т.е. их скалярное произведение равно нулю. Эти строки и составляют ансамбль $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ дискретных сигналов Уолша-Адамара $\Phi_i = (\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}})$, где n – размерность сформированной матрицы H_i (в IS-95 использованы H_i с $n = 64$).

Для передачи информации одна из строк $\Phi_i \in \Phi$ матрицы Адамара ставится в соответствие абонентскому каналу, например, для связи между базовой станцией и конкретным абонентом. Модуляция осуществляется по правилу (3), т.е. для передачи информационной "1" посылается строка Φ_i, для "0" – посылается последовательность, сформированная путем логического отрицания Φ_i (ее инверсная копия).

Для выделения сигнала на приемной стороне используется корреляционный приемник, т.е. вычисляется коэффициент корреляции (6). При точном совпадении начала пришедшей последовательности и имеющейся копии Φ_i наблюдаются пики корреляционной функции положительной и отрицательной полярностей – в зависимости от передаваемого бита. То есть, детектирование сигнала происходит следующим образом:

$$x(t) = \begin{cases} \text{"1", при } polarity > 0; \\ \text{"0", при } polarity < 0; \\ \text{сторонний сигнал, при } polarity = 0, \end{cases} \qquad (8)$$

где *polarity* – полярность пика корреляционной функции.

Таким образом, применение ортогональных систем дискретных сигналов Уолша-Адамара позволяет обеспечить высокоэффективную широкополосную цифровую связь. В тоже время число образуемых абонентских каналов связи не может превышать мощности M ансамбля сигналов, в данном случае оно не превышает размерности матрицы H_i, $M = n$. Другими словами, максимальное число возможных ортогональных кодов ограничено их длиной. Для рассмотренного примера имеем $M = 64$ (по спецификации IS-95 образуются 61 абонентский и 3 служебных канала). В этом смысле квазиортогональные дискретные сигналы (с $M > n$) имеют неоспоримое преимущество (см. таблицу 1), их применение потенциально позволит существенно повысить абонентскую мощность системы связи. Кроме того, для рассмотренных сигналов функция взаимной корреляции равна нулю лишь при отсутствии временного сдвига между последовательностями. Как следствие такие сигналы используются лишь в синхронных системах и преимущественно в прямых каналах (от базовой станции к абоненту).

Таким образом, перспективным направлением в развитии современных систем широкополосной связи с прямым расширением спектра является разработка и исследование методов синтеза больших ансамблей квазиортогональных дискретных сигналов с улучшенными ансамблевыми, структурными и корреляционными свойствами.

Рассмотренный подход к организации цифровых помехозащищенных каналов связи нашел применение при построении стеганографических методов защиты информации. Так, в работе [2] расширение спектра прямой последовательностью использовано для создания стеганографического метода встраивания данных в неподвижные изображения. Рассмотрим один из вариантов реализации этого метода, авторами которого являются Смит (J.R. Smith) и Комиски (B.O. Comiskey) [2], проведем исследования его эффективности с точки зрения обеспечиваемой пропускной способности стеганографического канала связи и достигаемой стойкости к несанкционированному извлечению информационных сообщений.

3. ПРЯМОЕ РАСШИРЕНИЕ СПЕКТРА В СТЕГАНОГРАФИИ

В методе Смита-Комиски [2], как и в рассмотренных выше системах связи с прямым расширением спектра, информационное сообщение побитно модулируется путем умножения на ансамбль ортогональных сигналов. Затем промодулированное сообщение встраивается в контейнер – неподвижное изображение.

Введем некоторые условные обозначения и математические соотношения, которые, по аналогии с рассмотренными выше системами широкополосной цифровой связи позволят исследовать особенности построения и информационного обмена данных в стеганосистеме.

Представим информационное сообщение m, подлежащее встраиванию в цифровой контейнер-изображение, в виде блоков m_i равной длины, т.е. $m = (m_0, m_1, ..., m_{N-1})$, где каждый блок m_i – последовательность (вектор) из n бит: $m_i = (m_{i_0}, m_{i_1}, ..., m_{i_{n-1}})$.

Контейнер-изображение будем рассматривать как массив данных C размерностью $K \cdot L$, разбитый на подблоки размером $k \cdot l = n$. В качестве элементов массива C могут выступать, например, растровые данные используемого изображения.

Секретными ключевыми данными является набор базисных функций

$$Key = \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\},$$

где все базисные функции $\Phi_i = (\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}})$ – взаимно ортогональные дискретные сигналы с

длиной, равной размеру n блока сообщения m_i, т.е. для любых $i, j \in [0,...,M-1]$ выполняется равенство

$$\rho\left(\Phi_i, \Phi_j\right) = \frac{1}{n}\sum_{z=0}^{n-1} \Phi_{i_z} \Phi_{jz} = \begin{cases} +1, \text{ при } i = j; \\ -1, \text{ при } i \neq j. \end{cases}$$

Формальное графическое представление информационного сообщения, контейнера-изображения и ключевых данных приведено на рис. 2.

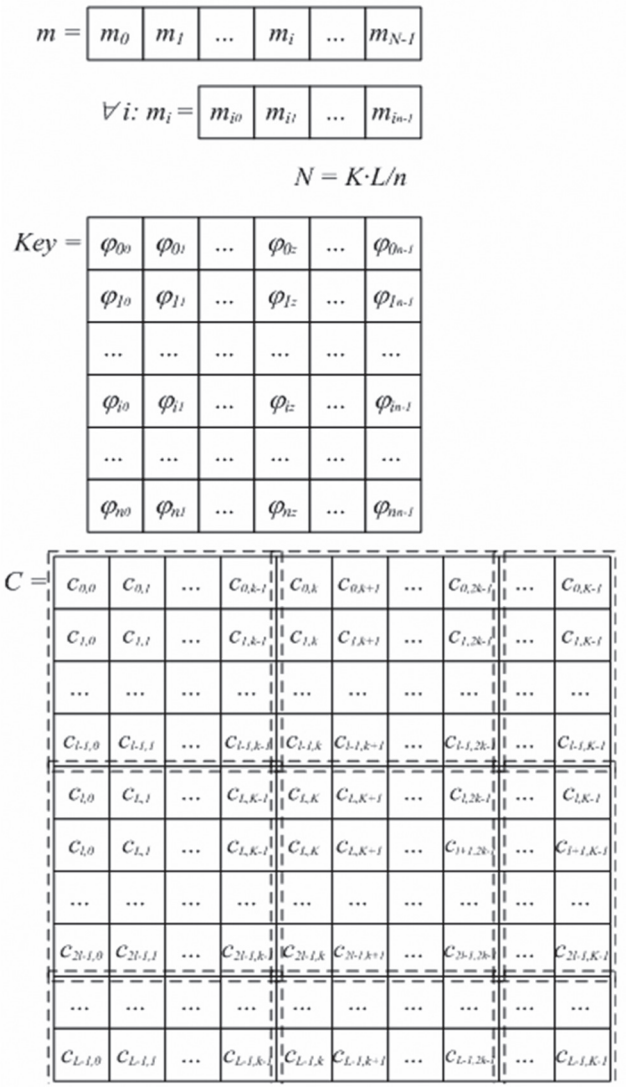


Рис. 2. Формальное представление информационного сообщения, контейнера-изображения и ключевых данных

Целью стеганографического преобразования информации является встраивание каждого отдельного блока сообщения m_i в соответствующий блок контейнера-изображения. В блок данных цифрового изображения размерностью $K \cdot L$ элементов может быть встроено $K \cdot \frac{L}{n}$ блоков информационного сообщения, т.е. до $K \cdot L$ битов.

Разбиение контейнера на блоки может быть произвольным, однако, как показывает практика, наиболее целесообразным (меньший, в отличие от одномерного представления, численный разброс значений в блоке) является двумерное разбиение, приведенное на рис. 2. В качестве ключевых данных (массива базисных функций $Key = \Phi$) будем использовать рассмотренные выше ансамбли ортогональных дискретных сигналов Уолша-Адамара.

Встраивание информационного сообщения осуществляется следующим образом. Каждый блок сообщения $m_{i_j}, j = 0,...,n-1$ сопоставляется с отдельным блоком контейнера-изображения. Каждый информационный бит блока $m_{i_j}, j = 0,...,n-1$ представляется в виде информационного сигнала

$$m_{i_j}(t) = \begin{cases} +1, m_{i_j} = 1; \\ -1, m_{i_j} = 0 \end{cases}$$

и по аналогии с (3) модулируется расширяющим кодовым сигналом (базисными функциями), т.е. ПСП .

В результате, для каждого информационного блока m_i формируется модулированный информационный сигнал

$$E_i(t) = \sum_{j=0}^{n-1}\sum_{z=0}^{n-1} m_{i_j}(t)\Phi_{j_z} . \qquad (9)$$

Полученный блок сообщения E_i попиксельно суммируется с подблоком контейнера.

Обозначим блоки контейнера следующим образом (см. рис. 3):

$$C_0 = \begin{pmatrix} c_{0,0} & c_{0,1} & \dots & c_{0,k-1} \\ c_{1,0} & c_{1,1} & \dots & c_{1,k-1} \\ \dots & \dots & \dots & \dots \\ c_{l-1,0} & c_{l-1,1} & \dots & c_{l-1,k-1} \end{pmatrix},$$

$$C_1 = \begin{pmatrix} c_{0,k} & c_{0,k+1} & \dots & c_{0,2k-1} \\ c_{1,k} & c_{1,k+1} & \dots & c_{1,2k-1} \\ \dots & \dots & \dots & \dots \\ c_{l-1,k} & c_{l-1,k+1} & \dots & c_{l-1,2k-1} \end{pmatrix}, \dots,$$

$$C_{N-1} = \begin{pmatrix} c_{L-l-1,K-k-1} & c_{L-l-1,K-k} & \dots & c_{L-l-1,K-1} \\ c_{L-l,K-k-1} & c_{L-l,K-k} & \dots & c_{L-l,K-1} \\ \dots & \dots & \dots & \dots \\ c_{L-1,K-k-1} & c_{l-1,k+1} & \dots & c_{L-1,K-1} \end{pmatrix}.$$

Соответствующие модулированные информационные сигналы $E_i(t)$ представим в виде двумерного массива данных:

$$E_i = \begin{pmatrix} E_{i_0} & E_{i_1} & \dots & E_{i_{k-1}} \\ E_{i_k} & E_{i_{k+1}} & \dots & E_{i_{2k-1}} \\ \dots & \dots & \dots & \dots \\ E_{i_{(l-1)(k-1)-k+1=n-k+1}} & E_{i_{(l-1)(k-1)-k+2=n-k+2}} & \dots & E_{i_{(l-1)(k-1)=n-1}} \end{pmatrix},$$

$$i = 0,..., N-1 .$$

Тогда стеганограмма (заполненный контейнер) формируется посредством объединения массивов данных S_i, $i = 0,..., N-1$:

$$S_i = C_i + E_i \cdot G, \quad (10)$$

где $G > 0$ – коэффициент усиления расширяющего сигнала, задающий «энергию» встраиваемых бит информационной последовательности.

Таким образом, заполненный контейнер S образуется из сформированных блоков S_i, $i = 0,...,N-1$ посредством их объединения как это показано на рис. 2 для исходного (пустого) контейнера C.

На этапе извлечения данных нет необходимости владеть информацией о первичном контейнере C. Операция декодирования заключается в восстановлении скрытого сообщения путем проецирования каждого блока S_i, полученного стеганоизображения S на все базисные функции $\Phi_j \in \Phi$, $i = 0,...,N-1$. Для этого каждый блок S_i представляется в форме вектора $S_i = \left(S_{i_0}, S_{i_1}, ..., S_{i_{n-1}}\right)$, $i = 0,...,N-1$.

Чтобы извлечь j-ый бит сообщения из i-го блока стеганоизображения, необходимо вычислить коэффициент корреляции между Φ_j и принятым блоком S_i (представленного в виде вектора):

$$\rho\left(S_i, \Phi_j\right) = \frac{1}{n}\sum_{z=0}^{n-1} S_{i_z} \Phi_{j_z} = \\ = G \cdot \frac{1}{n}\sum_{z=0}^{n-1} E_{i_z} \Phi_{j_z} + \frac{1}{n}\sum_{z=0}^{n-1} C_{i_z} \Phi_{j_z}, \quad (11)$$

где под C_i понимается одномерный массив, т.е. соответствующий блок контейнера, представленный в форме вектора.

Предположим, что массив C_i имеет случайную статистическую структуру, т.е. положим, что второе слагаемое в правой части выражения (11) близко к нулю и им можно пренебречь. Тогда имеем:

$$\rho\left(S_i, \Phi_j\right) \approx G \cdot E_i \cdot \Phi_j = G \cdot \sum_{l=0}^{n-1}\sum_{z=0}^{n-1} m_{i_x}(t) \cdot \Phi_{l_z} \Phi_{j_z}. \quad (12)$$

По аналогии с (6) отметим, что все последовательности из множества Φ взаимноортогональны, т.е. при $l \neq j$ имеем $\rho\left(\Phi_l, \Phi_j\right) = 0$. Следовательно, всеми слагаемыми в правой части равенства (12) при $l \neq j$ можно пренебречь. Отсюда имеем:

$$\rho\left(S_i, \Phi_j\right) \approx G \cdot m_{i_j}(t) \cdot \frac{1}{n}\sum_{z=0}^{n-1}\left(\Phi_{j_z}\right)^2 = G \cdot m_{i_j}(t). \quad (13)$$

По аналогии с выделением полезного сигнала (8) значения $m_{i_j}(t)$ могут быть легко восстановлены с помощью знаковой функции.

Поскольку $G > 0$ и $n > 0$ знак $\rho\left(S_i, \Phi_j\right)$ в (13) зависит только от $m_{i_j}(t)$, откуда имеем:

$$m_{i_j}(t) = \operatorname{sign}\left(\rho\left(S_i, \Phi_j\right)\right) = \begin{cases} -1, \text{ при } \rho\left(S_i, \Phi_j\right) < 0; \\ +1, \text{ при } \rho\left(S_i, \Phi_j\right) > 0; \\ ?, \text{ при } \rho\left(S_i, \Phi_j\right) = 0. \end{cases} \quad (14)$$

Если $\rho\left(S_i, \Phi_j\right) = 0$ в (14) будем полагать, что встроенная информация была утрачена.

Структурная схема встраивания информации в контейнер-изображение с использованием прямого расширения спектра для скрытной передачи сообщений представлена на рис. 3.

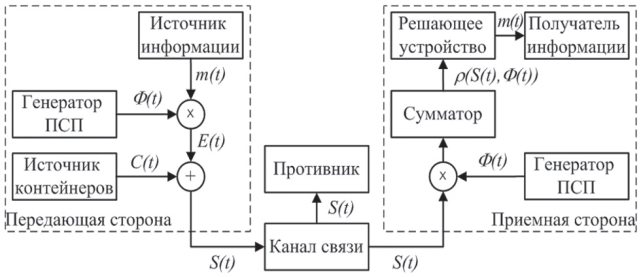


Рис. 3. Структурная схема встраивания информации в контейнер-изображение для скрытной передачи сообщений

Из рисунка следует, что процесс встраивания информационных сообщений для скрытной передачи очень похож на процесс расширения спектра дискретных сигналов в системах связи (см. рис. 1). Поэлементное сложение модулированного сообщения $E(t)$ с контейнером-изображением $C(t)$ (см. выражение (10)) следует интерпретировать как наложение ошибок $e(t)$ на полезный сигнал в канале связи $y(t)$. Задача извлечения сообщения $m(t)$ из $S(t)$ на приемной стороне стеганосистемы эквивалентна задаче детектирования $x(t)$ из смеси полезного сигнала и помехи $y'(t) = y(t) + e(t)$ в широкополосной системе связи. Другими словами, рассмотренная стеганосистема наследует все преимущества широкополосных систем связи: устойчивость к несанкционированному извлечению встроенных сообщений (аналог скрытности в системе связи), устойчивость к разрушению или модификации встроенных сообщений (аналог помехозащищенности), устойчивость к навязыванию ложных сообщений (аналог имитостойкости в системе связи).

Таким образом, использование прямого расширения спектра дискретных сигналов позволяет осуществить встраивание информационных данных в неподвижные изображения для скрытной передачи и реализовать, таким образом, стеганографическую защиту информации.

4. ОЦЕНКА ЭФФЕКТИВНОСТИ СТЕГАНОСИСТЕМЫ

Под эффективностью технической системы в широком смысле понимают соответствие результата выполнения некоторой операции требуемому. При этом техническая система выступает в роли средства реализации исследуемой операции.

Применительно к рассматриваемому процессу стеганографическая система выступает в роли технического средства реализации операции, целью которой является сокрытие от противника факта осуществления скрытной передачи информации. Таким образом, с учетом функционально-

го назначения стеганосистемы, введем следующие показатели эффективности.

1. *Пропускная способность* – отношение объема V встраиваемой в контейнер информации к общему объему D контейнера

$$Q = \frac{V}{D}. \qquad (15)$$

2. *Объем ключевых данных* (в битах)

$$l_{Key} = \log_2\left(|Key|\right), \qquad (16)$$

где $|Key|$ – мощность множества ключевых данных.

3. *Стойкость стеганографического метода* будем оценивать как величину, обратную мощности множества секретных ключевых данных. Ее можно трактовать как вероятностный показатель подбора секретного ключа:

$$W = \frac{1}{|Key|} = 2^{-l_{Key}}. \qquad (17)$$

4. *Величина вносимых искажений* как процентное отношение среднеарифметического всех абсолютных значений Δ-изменений данных контейнера к максимально возможному значению $\Delta_{\max}$:

$$I = \frac{\Delta_{cp}}{\Delta_{\max}} \cdot 100 = \frac{100}{\Delta_{\max} \cdot D} \cdot \sum_{i=1}^{D} |\Delta_i|, \qquad (18)$$

где Δ_i – Δ-изменения i-го элемента контейнера.

5. *Вероятность ошибочного извлечения* информационных данных сообщения

$$P_{ош} = \lim_{D\to\infty} \frac{V_{ош}}{D} = 1 - \lim_{D\to\infty} \frac{V - V_{ош}}{D}, \qquad (19)$$

где $V_{ош}$ – объем ошибочно извлеченных данных.

Используя показатели (15) – (19), оценим эффективность рассмотренного стеганографического метода защиты информации.

1. *Пропускная способность.* На каждый n-элементный блок S_i заполненного контейнера (стеганограммы) приходится n-битный вектор встроенного сообщения m_i (см. выражения (9), (10)). Следовательно, $Q = \frac{1}{B}$, где B – объем данных, приходящийся на один элемент контейнера. Для случая встраивания в растровые данные изображения (цветовая модель R,G,B) с 8-битным кодированием каждого цвета имеем $B = 8$ и $Q = \frac{1}{8}$.

2. *Объем ключевых данных.* Ключевыми данными является ансамбль дискретных сигналов, образованный строками матрицы Адамара порядка n. Следовательно, под множеством ключевых данных следует понимать множество различных (неизоморфных) матриц Адамара, каждая из матриц задает ансамбль дискретных сигналов. В [7] получены некоторые оценки мощности M_A этого множества, которые приведены в табл. 2.

Таблица 2

Число ансамблей дискретных сигналов Уолша-Адамара [7]

n	M_A
64	19
100	1
256	54
512	102
1024	162
2000	9
4000	16
10000	10

Приведенные оценки мощности M_A дают оценку числа ансамблей дискретных сигналов Уолша-Адамара, т.е. оценку мощности неэквивалентных ключей стеганосистемы. Следовательно, объем ключевых данных оценивается как $l_{key} = \log_2(M_A)$.

3. *Вероятность подбора* секретного ключа $W = (M_A)^{-1}$.

4. Для оценки *величины вносимых искажений* воспользуемся выражением (10). Второе слагаемое в правой части (10) определяет величину Δ-изменений элементов данных контейнера. Сомножитель E_i формируется в результате суммирования n дискретных сигналов (принимающих значения ± 1) с соответствующими полярностями (задаваемыми $m_{i_j}(t)$). Следовательно, все элементы E_i будут принимать значения из диапазона $[-n,...,+n]$, а соответствующие Δ-изменения элементов контейнера не будут превышать $|\Delta_i| \le n \cdot G$. Откуда имеем верхнюю оценку величины вносимых искажений:

$$I = \frac{\Delta_{cp}}{\Delta_{\max}} \cdot 100 \le \frac{n \cdot G}{\Delta_{\max}} \cdot 100. \qquad (20)$$

Для случая встраивания в растровые данные изображения (цветовая модель R,G,B) с 8 битным кодированием каждого цвета и использования дискретных сигналов с $n = 256$ даже при $G = 1$ вносимые искажения могут достигать 100%. Снизить вносимые искажения можно за счет сокращения числа встраиваемых бит данных m_{i_j} (уменьшив число слагаемых в (9)), что неизбежно приведет к снижению пропускной способности стеганографического канала связи.

5. *Вероятность ошибочного извлечения.* Извлечение информационного сообщения, также как и при организации помехозащищенной связи (см. (3) - (5)), осуществляется корреляционным способом (см. (11) – (14)). Следовательно, ошибка извлечения произойдет при изменении знака коэффициента корреляции $\rho(S_i, \Phi_j)$ в выражении (14).

Представим коэффициент $\rho(S_i, \Phi_j)$ в виде

$$\rho(S_i, \Phi_j) = \rho(C_i + E_i \cdot G, \Phi_j) = \rho(C_i, \Phi_j) + \rho(E_i \cdot G, \Phi_j).$$

Последнее слагаемое не изменяет знак $\rho(S_i,\Phi_j)$, событие

$$\rho(S_i,\Phi_j)=\rho(E_i\cdot G,\Phi_j)$$

соответствует безошибочному извлечению сообщения (см. (12), (13)).

Следовательно, ошибка извлечения информационного бита m_{i_j} сообщения произойдет при наступлении события

$$\left|\rho(C_i,\Phi_j)\right|>\rho\left|E_i\cdot G,\Phi_j\right|=\left|G\cdot m_{i_j}\right|=G\,, \qquad (21)$$

т.е. в том случае, когда абсолютное значение коэффициента корреляции используемого для встраивания бита m_{i_j} дискретного сигнала Φ_j с блоком контейнера C_i, в который этот бит встраивается, превзойдет коэффициент усиления G.

Таким образом, запишем

$$P_{ош}=P\left(\left|\rho(C_i,\Phi_j)\right|>G\right),$$

где $P(x)$ – вероятность наступления случайного события x.

Другими словами, правильное извлечение встроенного сообщения является случайным событием, вероятность $P_{б.ош}$ которого непосредственно связана со статистическими свойствами используемого контейнера-изображения. Для безошибочного извлечения сообщения

$$P_{ош}=0, P_{б.ош}=1-P_{ош}=1, \qquad (22)$$

следует стремиться к взаимной ортогональности отдельных фрагментов изображения C_i и используемых в качестве секретных ключей дискретных сигналов Φ_j. В этом случае событие

$$\left|\rho(C_i,\Phi_j)\right|=0<G\,,$$

для всех $i=0,...,N-1$ является достоверным и выполняется (22).

В тоже время, как показали экспериментальные исследования, коэффициент корреляции, как правило, значительно больше нуля $\left|\rho(C_i,\Phi_j)\right|>>0$ и очень часто возникает событие (21). Дело в том, что элементы дискретных сигналов $\Phi_j\in\Phi$ принимают значения $\begin{cases}+1\\-1\end{cases}$, а соответствующий нормированный коэффициент корреляции $\rho\left(\Phi_i,\Phi_j\right)$ по абсолютному значению не превосходит длины n последовательности (см. (2)) и лежит в диапазоне $[0,...,1]$, откуда собственно и следует условие (21).

Однако элементы контейнера C_i принимают значение из числового поля $[0,...,Y]$, размерность которого задается способом кодирования данных изображения. Например, при встраивании информации в растровые данные изображения (цветовая модель R,G,B) с 8 битным кодированием каждого цвета соответствующие C_i принимают значения из диапазона целых чисел $[0,...,255]$. Другими словами, абсолютное значение нормированного относительно n коэффициента корреляции $\left|\rho(C_i,\Phi_j)\right|$ будет лежать в диапазоне $[0,...,Y]$ и для безошибочного извлечения всех битов сообщения (21) необходимо выполнить условие $G>Y$.

В тоже время повышение G ведет к неизбежному росту величины вносимых искажений (20), которые при $I>2...3\%$ (порог зрительной чувствительности человека) становятся заметны стороннему наблюдателю [1, 2], что компрометирует стеганоканал и делают невозможным использование рассмотренной стеганосистемы.

Таким образом, в ходе исследований выявлены следующие противоречия, лежащие в основе разработки и использования стеганографических систем с расширением спектра дискретных сигналов:

– вероятность правильного извлечения встроенных данных $P_{б.ош}$ лежит в прямой зависимости от величины вносимых искажений I;

– величина вносимых искажений I лежит в прямой зависимости от объема встраиваемых бит данных, т.е. от пропускной способности стеганоканала Q;

– вероятность правильного извлечения встроенных данных $P_{б.ош}$ непосредственно зависит от статистических свойств используемого контейнера-изображения.

Для экспериментального исследования эффективности рассмотренного метода встраивания сообщений в неподвижные изображения разработана программная реализация, получены следующие эмпирические оценки:

– зависимости величины вносимых искажений I от пропускной способности Q стеганоканала;

– зависимости величины вносимых искажений I и частоты ошибок извлечения $P^*_{ош}\approx P_{ош}$ от коэффициента усиления G;

– зависимости величины вносимых искажений I от частоты ошибок извлечения $P^*_{ош}\approx P_{ош}$.

Исследования проводились при встраивании информационных данных в растровые данные изображения (цветовая модель R,G,B) с 8 битным кодированием каждого цвета. Полученные эмпирические зависимости приведены на рис. 4–7.

Анализ экспериментально полученных зависимостей подтверждает сделанные ранее выводы, сходимость результатов эксперимента с теоретическими рассуждениями свидетельствует о достоверности полученных результатов.

Из приведенной на рис. 4. зависимости следует, что повышение пропускной способности стеганоканала ведет к резкому увеличению вносимых искажений в контейнер-изображение. Незаметные для стороннего наблюдателя искажения (лежащие ниже порога чувствительности зрительной системы человека) вносятся лишь при $Q\le 0{,}005$. Это соответствует встраиванию не более 10 битов в один блок изображения, т.е. модулированию до десяти информационных сигналов $m_{i_j}(t)$, $j=0,...,9$ в выражении (9).

Зависимости, приведенные на рис. 5, 6, свидетельствуют, что коэффициент усиления, используемый в выражениях (10) – (13), позволяет существенно снизить вероятность ошибочного извлечения информационных данных. К сожалению, это достигается за счет резкого повышения вносимых искажений в используемый контейнер-изображение. Зависимости получены при $Q = 0{,}005$. Очевидно, что для такой величины пропускной способности коэффициент усиления не может превосходить 1 .. 1,5 (см. рис. 5). Однако даже для таких значений вероятность ошибочного извлечения велика и лежит в диапазоне 0,1 .. 0,5.

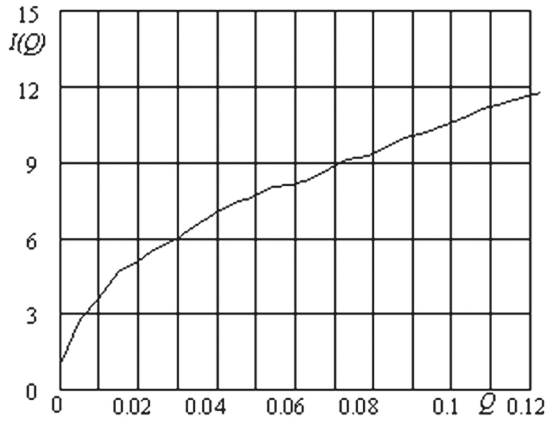


Рис. 4. Зависимость $I(Q)$

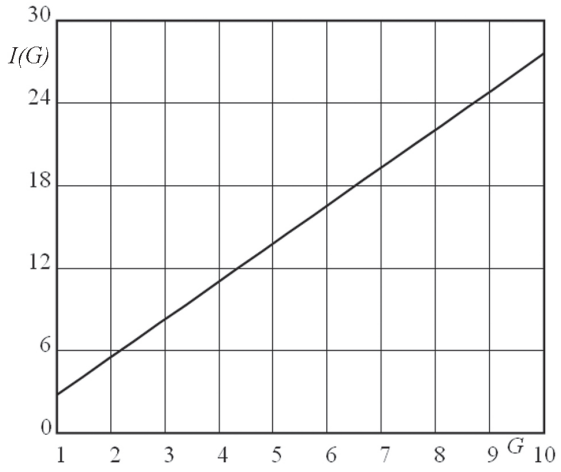


Рис. 5. Зависимость $I(G)$ при $Q = 0{,}005$

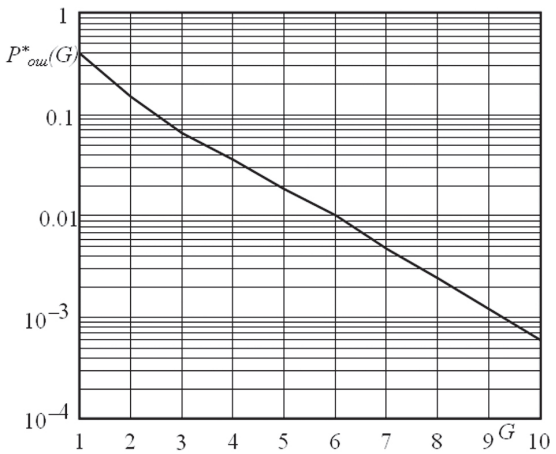


Рис. 6. Зависимость $P^*_{ош}(G)$ при $Q = 0{,}005$

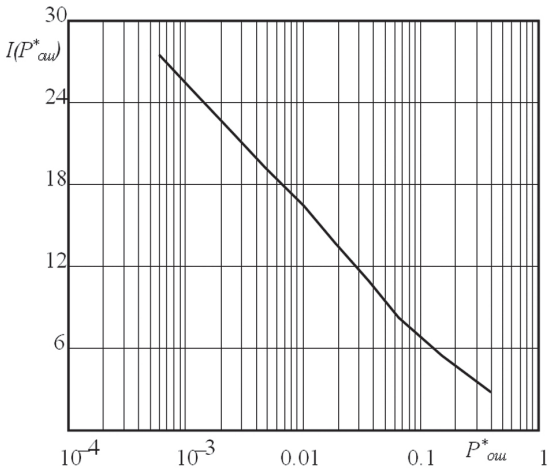


Рис. 7. Зависимость $I(P^*_{ош})$ при $Q = 0{,}005$

Интегральная зависимость $I(P^*_{ош})$, приведенная на рис. 6, обобщает приведенные на рис. 5, 6 данные. Для фиксированной пропускной способности $Q = 0{,}005$ получена эмпирическая кривая, характеризующая зависимость величины вносимых искажений в контейнер-изображение и вероятности ошибочного извлечения информационных данных. Для $Q = 0{,}005$ добиться низких искажений, лежащих ниже порога зрительной чувствительности человека ($I \le 2...3\%$), можно только при очень высокой вероятности ошибочного извлечения информационных данных ($P_{ош} \ge 0{,}1$). Очевидно, что практическое применение подобных стеганосистем необходимо сочетать с помехоустойчивым кодированием информационных данных, что позволит существенно снизить $P_{ош}$.

ВЫВОДЫ

В результате проведенных исследований показано, что использование в стеганографических целях прямого расширения спектра дискретных сигналов позволяет осуществить скрытное встраивание информационных сообщений в неподвижные изображения. Задача извлечения сообщения на приемной стороне стеганосистемы эквивалентна задаче обнаружения информации из смеси полезного сигнала и помехи в широкополосной системе связи.

В ходе исследований выявлены следующие недостатки стеганографических систем с расширением спектра дискретных сигналов: вероятность правильного извлечения встроенных данных зависит от величины вносимых искажений, которая в свою очередь зависит от обеспечиваемой пропускной способности стеганоканала. Иначе говоря, практическое построение стеганосистемы сопряжено с поиском компромисса между величиной вносимых искажений, вероятностью правильного извлечения сообщения на приемной стороне и обеспечиваемой пропускной способностью. Кроме того, в ходе исследований установлено, что вероятность правильного извлечения встроенных данных непосредственно

зависит от статистических свойств используемого контейнера-изображения.

Перспективным направлением дальнейших исследований, по мнению авторов, является использование больших ансамблей слабокоррелированных (квазиортогональных) дискретных сигналов для построения стеганосистем с прямым расширением спектра. Это позволит, с одной стороны, без значительного повышения вносимых искажений в контейнер-изображение существенно повысить пропускную способность стеганоканала. С другой стороны, за счет адаптивного формирования (выбора) дискретных сигналов по критерию минимизации коэффициента корреляции с контейнером изображением это позволит существенно снизить вероятность ошибочного извлечения встроенных данных.

Литература.

[1] *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс», 2006. – 288 с., ил.

[2] *J. Smith, B. Comiskey,* Modulation and Information hiding in Image. // Information hiding: First Int. Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol 1174. 1996. – pp. 207-227.

[3] Цифровые методы в космической связи. /Под ред. С. Голомба.- М.: Связь, 1969. – 272 с.

[4] *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

[5] *Горбенко И.Д., Стасев Ю.В.* Анализ производных ортогональных систем сигналов // Радиотехника. – 1989. – № 9. – С. 16 – 18.

[6] *Стасев Ю.В., Кузнецов А.А., Носик А.М., Качур Л.Н.* Формирование больших ансамблей дискретных сигналов с использованием избыточных кодов // Збірник наукових праць ХУПС. – Харків: ХУПС. – 2008. – Вип. 2 (17). – С. 102-109.

[7] *Стасєв Ю.В.* Основи теорії побудови сигналів. – Х.: ХВУ, 1999. – 87с.

Поступила в редколлегию 5.07.2010.

Кузнецов Александр Александрович, доктор технических наук, профессор, профессор кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория обработки и передачи данных, стеганографические методы защиты информации.

Ботнов Антон Михайлович, студент 5 курса факультета компьютерной инженерии и управления ХНУРЭ. Область научных интересов: методы обработки и передачи данных, стеганографические методы защиты информации.

Лаптий Павел Александрович, студент 5 курса факультета компьютерной инженерии и управления ХНУРЭ. Область научных интересов: методы обработки и передачи данных, стеганографические методы защиты информации

УДК 519:616-079.4:616.5

Вбудовування інформаційних даних в нерухомі зображення з використанням прямого розширення спектру / О.О. Кузнєцов, д.т.н., проф., А.М. Ботнов, П.О. Лаптій / / Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 470-478.

У статті досліджуються стеганографічні методи захисту інформації на основі прямого розширення спектра дискретних сигналів. Пропонується стеганографічний метод приховування даних в нерухоме зображення з використанням квазіортогональних дискретних сигналів. Показано, що запропонований метод дозволяє підвищити пропускну здатність стеганографічного каналу зв'язку та зменшити частку спотворень, що вносяться в контейнер-зображення.

Ключові слова: метод розширення спектру, дискретний сигнал, кореляційний прийом, стеганографічний захист інформації.

Табл. 02. Іл. 06. Бібліогр.: 7 найм.

UDC 519:616-079.4:616.5

Data embedding in stationary images by using direct spectrum expansion / A.A Kuznetsov, A.M Botnov, P.A. Laptii // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 470-478.

Stenographic methods of embedding data into stationary images for secretive information transmission are considered. The paper considers the method of stenographic protection based upon the use of the direct expansion of a spectrum of discrete signals, investigates, its efficiency from the point of view of provided strength, capacity and magnitude of distortions entered in a container-image.

Key words: spectrum expansion method, discrete signal, correlation reception, steganographic data protection.

Tab. 02. Fig. 06. Ref.: 7 items.

УДК 681.3.06

МЕТОДИ ПОБУДОВИ ТА ВЕРИФІКАЦІЇ НЕСУПЕРЕЧНОСТІ І ПОВНОТИ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

О.В. ПОТІЙ, А.В. ЛЄНШИН

Проведено аналіз вимог нормативних документів в частині формування профілів захищеності. Визначені недоліки існуючого підходу до формування профілю захищеності. Сформульовані вимоги до методу формування та методу верифікації несуперечності і повноти профілів захищеності, надано їх опис. Показано, що розроблені методи відповідають вимогам із: часової складності, стандартизованості підходу (повторюваність і порівнюваність результатів), несуперечності нормативним документам, зрозумілості проміжних результатів та їх впливів на остаточний вибір, а також можливості самоперевірки особи, що використовує метод.

Ключові слова: профіль захищеності, несанкціонований доступ, методи системного аналізу.

ВСТУП

Захист інформації з обмеженим доступом, а також інформації, захист якої гарантується державою, має здійснюватися за рахунок створення комплексної системи захисту інформації (далі – КСЗІ) [1]. Основним документом, що регламентує порядок розробки та впровадження КСЗІ, є технічне завдання. Технічне завдання має містити вимоги із захисту від несанкціонованого доступу (далі – НСД), а також витоку інформації технічними каналами. Для того, щоб викласти вимоги із захисту від НСД, в Україні використовується механізм функціональних профілів захищеності (далі – ФПЗ) від НСД, що мають відповідати вербальній та/або формалізованій політиці безпеки комплексу засобів захисту комп'ютерної системи (далі – КС). У вітчизняній літературі під КС розуміється сукупність програмно-апаратних засобів, яка подана для оцінки. Тобто фактично КС є аналогом об'єкта оцінки (ТОЕ – Target Of Evaluation) за ISO/IEC 15408, відомого під назвою "Єдині критерії".

На відміну від міжнародного стандарту ISO/IEC 15408, вітчизняні документи системи технічного захисту інформації, на жаль, не містять практичних рекомендацій щодо порядку вибору функціональних послуг безпеки, що мають задовольнити цілям безпеки конкретної організації. Ось чому, сучасний український фахівець при проектуванні системи захисту інформації власноруч має боротися із проблемою відсутності науково-обґрунтованої методики розробки ФПЗ, яка б забезпечувала не лише такі важливі властивості, як порівнюваність та повторюваність результатів експертизи, але б і надавали засоби самоперевірки та інтеграції з іншими процесами зі створення КСЗІ. Єдиним механізмом, що незважаючи на свою недосконаліть закріплений у нормативних документах України, є механізм стандартних ФПЗ, що рекомендовані до використання у автоматизованих системах різного класу (відокремленої, однокористувацької робочої станції, локальної обчислювальної мережі чи розподіленої системи із передачею інформації через глобальну мережу Інтернет).

Аналіз підходу закріпленого у НД ТЗІ 2.5-004-99 показав, що використання стандартних ФПЗ можливо лише у якості відправної точки, що полегшує вибір узгодженого набору функціональних послуг для КС, що функціонує у складі автоматизованої системи певного класу. Проте, у разі необхідності врахування конкретних загроз, чи недоцільності (наприклад, з економічної точки зору) використання певної послуги безпеки виникають завдання, розв'язання яких за обсягом не поступається розробці ФПЗ з "нуля".

Зважаючи на вищезазначене, було поставлено таку ціль роботи: проаналізувати існуючи підходи до формування ФПЗ та розробити методи, які б дозволили не лише формувати ФПЗ, але і перевіряти несуперечність запропонованих варіантів та достатність послуг безпеки, що входять до складу ФПЗ. У цій статті наводяться основні результати проведених досліджень та ставляться завдання на подальше вдосконалення запропонованих методів.

1. ДОСЛІДЖЕННЯ ПІДХОДІВ З РОЗРОБКИ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ В УКРАЇНІ

У 1999 році в Україні введено в дію НД ТЗІ 2.5-004-99 [2], який визначає критерії оцінки захищеності КС від НСД та НД ТЗІ 2.5-005-99 [3], що надає нормативно-методологічну базу для вибору та реалізації вимог із захисту інформації в АС. Незважаючи на те, що минуло 11 років, а підходи до проектування та оцінювання систем захисту інформації пройшли кілька етапів еволюційного розвитку (це підтверджується наявністю вже третьої версії всесвітньо-визнаного аналогу зазначених документів – ISO/IEC 15408) в Україні ці документи не переглядалися жодного разу.

Важливим кроком у цьому напрямку, на нашу думку, є прийняття НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09, що призначені для оцінювання функціональних послуг безпеки, оцінювання рівня

гарантій коректності реалізації функціональних послуг безпеки. Але поза кадром на сьогодні залишилося питання, яким чином первинно обґрунтувати склад ФПЗ. Основним призначенням НД ТЗІ 2.5-004-99 є надання порівняльної шкали для оцінки надійності механізмів захисту та орієнтирів для розробки КС із функціями захисту інформації. Слід зауважити, що функціональні послуги з НД ТЗІ 2.5-004-99 мають по кілька рівнів, які у загальному випадку знаходяться у ієрархічній залежності (у сенсі рівня захисту, що забезпечується від загроз певного типу).

Сукупність критеріїв щодо реалізації функціональної послуги безпеки на певному рівні подані у табличному вигляді, рядки таблиці фактично є специфікаціями, наявність яких є достатньою для підтвердження реалізації у КЗЗ певного рівня заданої послуги безпеки.

У табл. 1 наведено формалізоване подання специфікації на прикладі послуги "Довірча конфіденційність". У таблиці 1 не вказані конкретні вимоги, а використовуються лише такі позначення: знак "+" на перетині рядка (що вказує на специфікацію) та стовпця (що визначає рівень послуги) позначає, що відповідна специфікація є обов'язковою для визначеного рівня послуги, знак "–" вказує на відсутність необхідності реалізації вимог відповідної специфікації, а об'єднані комірки позначають, що вимоги не відрізняються для рівнів послуг, що визначаються відповідними стовпцями.

У документі [3] визначено підхід до визначення ФПЗ шляхом вибору з множини стандартних ФПЗ. Зважаючи на те, що цей підхід є єдиним, що визначений у НД ТЗІ та для спрощення викладення матеріалів, далі у статті використовується термін "стандартний підхід". Стандартний підхід базується на таких припущеннях:

а) Усі АС можна віднести до одного з трьох класів за наступними ознаками: конфігурація апаратних засобів, їх фізичне розміщення, кількість категорій оброблюваної інформації, кількість користувачів і категорій користувачів.

б) У межах класу АС можна віднести до одного з підкласів, що визначені за критерієм необхідності забезпечення: конфіденційності, цілісності та доступності інформації. Таким чином, кількість сполучень з трьох властивостей зумовлює наявність семи підкласів АС (табл. 2).

в) Вимоги до безпеки АС різних класів суттєво відрізняються, що дозволяє сформувати для їх підкласів множини стандартних ФПЗ, що знаходяться у ієрархічній залежності (реалізація забезпечує наростаючу захищеність від загроз певного типу).

г) Для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Визначено такі етапи застосування стандартного підходу для визначення ФПЗ для КС, що використовується у складі АС.

Е1) Визначення класу АС. Е2) Визначення, яке сполучення вимог конфіденційності, цілісності, доступності висувається до АС. Е3) Визначення призначення АС та вибір підказки ("маски"), яку треба використовувати у цьому випадку для вибору одного зі стандартних ФПЗ (використовуючи довідковий додаток А з НД ТЗІ 2.5-005-99). Якщо призначення АС відрізняється від наведених у [3], необхідно власноруч обрати підмножину стандартних ФПЗ, відповідно до класу АС, у якій експлуатується КС. Е4) Аналіз сутності вимог, відібраних стандартних ФПЗ. Е5) Вибір одного зі стандартних ФПЗ, що найбільш відповідає політиці безпеки КЗЗ КС. Е6) У випадку, коли жоден із стандартних ФПЗ не підходить повною мірою, необхідно змінити рівень послуги, що міститься у стандартному ФПЗ, або додати нову послугу. При цьому необхідно врахувати залежності між послугами, що визначені у НД ТЗІ 2.5-004-99.

Визначимо переваги та недоліки, що притаманні стандартному підходу. Основними перевагами є відносна простота за рахунок: наявності готових шаблонів ФПЗ для КС, можливості звуження простору вибору за рахунок визначення призначення АС (автоматизації діяльності органів державної влади, автоматизації банківської діяльності, керування технологічними процесами, довідково-пошукові системи), до складу якої входять КС, врахування необхідних зв'язків між послугами, що входять до складу стандартних ФПЗ. До основних недоліків слід віднести: значну

Таблиця 1

Приклад специфікації послуги "Довірча конфіденційність" з НД ТЗІ 2.5-004-99

Специфікація \ Рівні послуги	КД-1	КД-2	КД-3	КД-4
Множина об'єктів, яких стосується політика послуги	+		+	
Атрибути доступу, що використовує КЗЗ	+	+		+
Обробка запитів на зміну прав доступу	+	+	+	+
Правила керування доступом до об'єктів домену	+	+	+	+
Правила керування доступом до процесів домену	–	+	+	
Початкові права доступу та правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	+			
Необхідні умови (залежності послуги)	НИ-1		КО-1, НИ-1	

складність (особливо часову) детального аналізу послуг безпеки, що входять до складу стандартних ФПЗ, відсутність формалізованого (та зрозумілого користувачу) зв'язку між включеними до стандартного ФПЗ послугами безпеки (їх рівнями) та загрозами і ризиками для конкретної КС. Власне кажучи, недоліки стандартного методу є наслідком його основної переваги. Стандартний ФПЗ не може повністю відповідати вимогам довільної КС, якщо кількість стандартних ФПЗ не дорівнює загальній кількості можливих ФПЗ, а у випадку рівності цих величин це вже не стандартні ФПЗ, а "припустимі профілі". Звісно, що використання у стандартному підході "припустимих профілів" призвело б до надвеликої складності їх належного аналізу. Кількість стандартних ФПЗ для окремих підкласів [3] визначені у табл. 2.

Таблиця 2

Результати кількісного аналізу стандартних ФПЗ з НД ТЗІ 2.5-005-99

Клас АС	Кількість стандартних ФПЗ для підкласів АС							Загальна кількість стандартних ФПЗ
	К	Ц	Д	КЦ	КД	ЦД	КЦД	
АС-1	2	2	4	2	4	4	4	22
АС-2	6	5	4	6	4	4	5	34
АС-3	6	5	4	6	4	4	5	34

Проведений аналіз [2] показав, що послуги безпеки вважаються більш-менш незалежними, за небагатьма виключеннями: послуга НЦ (цілісність КЗЗ) перший рівень якої, тобто НЦ-1, є обов'язковим для реалізації усіх інших послуг безпеки, а також деякими іншими залежностями, основними з яких є необхідність у реалізації послуг НО (розподіл обов'язків) та НИ (ідентифікація та автентифікація). Як видно з припущення б) щодо стандартного методу така властивість інформації як "спостереженість" не використовується для розбиття АС на підкласи. У роботі [3] цей факт пояснюється тим, що послуги спостереженості є необхідною умовою для реалізації інших послуг, а з іншого боку завжди важлива для КС. Проте швидше за все, не внесення властивості "спостережність" як такої, що визначає підклас, зумовлено тим, що розробники намагалися зменшити обсяг роботи особи, яка приймає рішення (ОПР) щодо вибору ФПЗ за рахунок зменшення кількості стандартних ФПЗ.

2. ДОСЛІДЖЕННЯ НЕСУПЕРЕЧНОСТІ ТА ДОСТАТНОСТІ СТАНДАРТНИХ ФПЗ, ЩО ВИЗНАЧЕНІ У НД ТЗІ 2.5-005-99

Перед тим як викласти результати дослідження несуперечності та достатності стандартних ФПЗ наведемо семантику їх опису, як вона визначається у НД ТЗІ 2.5-005 -99:

1.Д.4 = {ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2}. (1)

Опис профілю складається з трьох частин: буквено-числового ідентифікатора, знака рівності і переліку рівнів послуг, взятого в фігурні дужки. Ідентифікатор у свою чергу включає: позначення класу АС (1, 2 або 3), буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д), номер профілю і необов'язкове буквене позначення версії. Всі частини ідентифікатора відділяються один від одного крапкою.

Як визначається НД ТЗІ 2.5-005-99: "Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ ОС, проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків." Отже для розробки ФПЗ для конкретної КС необхідно проведення аналізу та оцінки ризиків є обов'язковим.

Задамо собі питання: "Яку частину можливого простору припустимих варіантів ФПЗ покривають стандартні ФПЗ?". Для надання відповіді обчислимо граничні значення кількості "припустимих" ФПЗ із застосуванням комбінаторного підходу. Нехай існує множина $\{abcd\}$, така, що $a=\overline{1,N_a}$, $b=\overline{1,N_b}$, $c=\overline{1,N_c}$, $d=\overline{1,N_d}$, тоді кількість можливих варіантів розраховуватиметься як:

$$M_{abcd} = N_a \cdot N_b \cdot N_c \cdot N_d . \qquad (2)$$

Розглянемо кілька прикладів для ілюстрації способу застосування виразу (2).

Приклад 1:

Нехай: $N_a = N_b = N_c = N_d = 10$, тоді кількість можливих варіантів: $M_{abcd} = 10^4$ (0-9999). Такий результат легко зрозумілий, оскільки така множина дорівнює діапазону десяткових цифр чотиризначного PIN-коду, з яким кожен з нас зустрічається у повсякденній практиці використання кредитних карток.

Приклад 2:

Нехай: $N_a = 2, N_b = 2, N_c = 3$, тоді кількість можливих варіантів: $M_{abcd} = 2 \cdot 2 \cdot 3 = 12$ (дивись дані таблиці 3).

Таблиця 3

Множина варіантів комбінацій для прикладу 2

A	b	c
1	1	1
1	1	2
1	1	3
1	2	1
1	2	2
1	2	3

a	b	c
2	1	1
2	1	2
2	1	3
2	2	1
2	2	2
2	2	3

Розглянувши ці прості приклади, можна безпосередньо перейти до розрахунку нижньої (S_L) та верхньої (S_H) границі кількості "припусти-

мих" ФПЗ. Для обчислення нижньої границі нам необхідно знати кількість рівнів для кожної i – й послуги безпеки, тобто знати множину $\{N_i\}, i=\overline{1,I}$, де I - загальна кількість послуг безпеки (для випадку НД ТЗІ 2.5-004-99: $I=22$). Використовуючи вираз (2) та дані таблиці 4, маємо, що $S_L \approx 7\cdot 10^9$ варіантів. Така оцінка справедлива, якщо ми вважатимемо, що в довільному ФПЗ обов'язково мають бути представлені усі функціональні послуги, але такої вимоги не висувається, тому кількість можливих рівнів для кожної i-ої послуги (враховуючи нульовий рівень, коли послуги відсутні у ФПЗ) дорівнюватиме $N_i^+ = N_i + 1$. Отже $S_H \approx 6{,}3\cdot 10^{12}$. Вихідні дані та результати розрахунків зведені до табл. 4.

Таблиця 4

Розрахунок верхньої та нижньої границі кількості можливих ФПЗ

i	Послуга	N_i	N_i^+	i	Послуга	N_i	N_i^+
1	КД	4	5	12	ДЗ	3	4
2	КА	4	5	13	ДВ	3	4
3	КО	1	2	14	НР	5	6
4	КК	3	4	15	НИ	3	4
5	КВ	4	5	16	НК	2	3
6	ЦД	4	5	17	НО	3	4
7	ЦА	4	5	18	НЦ	3	3*
8	ЦО	1	2	19	НТ	3	4
9	ЦВ	3	4	20	НВ	3	4
10	ДР	3	4	21	НА	2	3
11	ДС	3	4	22	НП	2	3
Кількість варіантів							
Нижня границя:		7 255 941 120		Верхня границя:		6 370 099 200 000	

* Оскільки будь-який ФПЗ має включати послугу НЦ, послуга не має нульового рівня.

Розгляд НД ТЗІ 1.1-002-99 "Загальні положення про захист інформації в КС від НСД" показує, що при наданні послуг конфіденційності та цілісності може бути використаний довірчий або адміністративний принципи керування доступом.

Під довірчим керуванням доступом слід розуміти таке керування, при якому засоби захисту дозволяють звичайним користувачам управляти (довіряють керування) потоками інформації між іншими користувачами і об'єктами свого домену (наприклад, на підставі права володіння об'єктами), тобто призначення і передача повноважень не вимагають адміністративного втручання.

Адміністративне керування доступом – керування, при якому керувати потоками інформації між користувачами та об'єктами дозволено лише адміністраторам (авторизованим користувачам).

Не важко помітити, що ці принципи є взаємовиключними, тобто не можуть одночасно застосовуватися до одного і того ж об'єкта. Множини об'єктів КС, до якої мають застосовуватися послуги з довірчим чи адміністративним принципом керування доступу, зведені до табл. 5.

У ході дослідження несуперечності стандартних ФПЗ було з'ясовано, що деякі з них вказують на необхідність одночасного застосування послуг, що базуються на різних принципах керування доступом, але відносяться до всіх об'єктів КС. Результати проведеного аналізу з врахування семантики ФПЗ та даних табл. 5 зведені до табл. 6.

Таблиця 5

Визначення множини об'єктів для послуг КД, КА, ЦД, ЦА

№	Рівні послуги	Політика ПОСЛУГИ, що реалізується КЗЗ, повинна
1	КД–1, КД-2, ЦД-1, ЦД-2, КА–1, КА-2, ЦА-1, ЦА-2	визначати множину об'єктів КС, до яких вона відноситься
2	КД–3, КД-4, ЦД-3, ЦД-4, КА–3, КА-4, ЦА-3, ЦА-4	відноситись до всіх об'єктів КС

Підводячи підсумки вищенаведеного, можна стверджувати, що:

– стандартні ФПЗ перекривають незначну частину простору припустимих ФПЗ;

– у стандартних ФПЗ присутні неточності типу "друкарські помилки" та "несумісне використання рівнів послуг";

– згідно рекомендацій з НД ТЗІ 2.5-005-99 для побудови адекватної загрозам системи захисту обов'язково необхідно здійснювати аналіз ризиків, результати якого мають використовуватися для уточнення чи розробки ФПЗ;

– уточнення стандартного ФПЗ за складністю можна порівняти з формуванням ФПЗ наново.

3. МЕТОД ПОБУДОВИ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ВІД НСД

Проведений у першому розділі аналіз та недоліки стандартного підходу дозволив сформулювати такі вимоги до методу, що розробляється [4]:

– зручність застосування (В1);

– зрозумілість проміжних результатів та їх впливу на остаточний склад ФПЗ (В2);

– врахування вимог нормативних документів у сфері ТЗІ (В3);

– коректність переходів між різними етапи визначення складу ФПЗ (В4);

– можливість самоперевірки ОПР (В5);

– наявність формалізованого процесу вибору та можливість використання результатів для документування ходу вибору елементів ФПЗ (В6);

– можливість інтеграції з іншими етапами побудови КСЗІ (В7).

Під В1 розуміється, логічність та ненадлишковість викладення текстової частини та використання у методі допоміжного інструментарію (наприклад, опитувальних листів, таблиць, формул, рисунків), що дозволять ОПР зосередитися на виконанні безпосередньо вирішуваної задачі

Таблиця 6

Стандартні ФПЗ, що не задовольняють висунутим вимогам

№	СФПЗ	Зауваження
1	1.К.1	Не зрозуміло, яким чином забезпечується конфіденційність інформації, що обробляється, оскільки послуги конфіденційності відсутні у СФПЗ
2	1.Ц.1	Не зрозуміло, яким чином забезпечується цілісність інформації, що обробляється, оскільки послуги цілісності відсутні у СФПЗ
3	1.КЦ.1	Не зрозуміло, яким чином забезпечується конфіденційність та цілісність інформації, що обробляється, оскільки послуги конфіденційності та цілісності відсутні у СФПЗ
4	2.К.5	Одночасна наявність послуг: КД-3, КА-3 є неможливою
5	2.К.6	Одночасна наявність послуг: КД-4, КА-4 є неможливою
6	2.Ц.5	Одночасна наявність послуг: ЦД-4, ЦА-4 є неможливою
7	2.КЦ.5	Одночасна наявність послуг: КД-3, КА-3 є неможливою
8	2.КЦ.6	Одночасна наявність послуг: КД-4, КА-4 та ЦД-4, ЦА-4 є неможливою
9	2.КД.3	Одночасна наявність послуг: КД-3, КА-3 є неможливою
10	2.КД.4	Одночасна наявність послуг: КД-4, КА-4 є неможливою
11	2.ЦД.4	Одночасна наявність послуг: ЦД-4, ЦА-4 є неможливою
12	2.КЦД.4	Одночасна наявність послуг: КД-3, КА-3 є неможливою
13	2.КЦД.5	Одночасна наявність послуг: КД-4, КА-4 та ЦД-4, ЦА-4 є неможливою
14	3.К.5	Одночасна наявність послуг: КД-3, КА-3 є неможливою
15	3.К.6	Одночасна наявність послуг: КД-4, КА-4 є неможливою
16	3.Ц.5	Одночасна наявність послуг: ЦД-4, ЦА-4 є неможливою
17	3.КЦ.5	Одночасна наявність послуг: КД-3, КА-3 є неможливою
18	3.КЦ.6	Одночасна наявність послуг: КД-4, КА-4 та ЦД-4, ЦА-4 є неможливою
19	3.КД.3	Одночасна наявність послуг: КД-3, КА-3 є неможливою
20	3.КД.4	Одночасна наявність послуг: КД-4, КА-4 є неможливою
21	3.ЦД.4	Одночасна наявність послуг: ЦД-4, ЦА-4 є неможливою
22	3.КЦД.4	Одночасна наявність послуг: КД-3, КА-3 є неможливою
23	3.КЦД.5	Одночасна наявність послуг: КД-4, КА-4 та ЦД-4, ЦА-4 є неможливою

– виборі елементів ФПЗ, а не на вивченні особливостей методу.

Під В2 розуміється можливість ОПР відстежувати, яким чином її вибір на певному кроці впливає на проміжні/остаточні результати. Реалізація цієї вимоги необхідна для більшого залучення та творчої реалізації потенціалу ОПР, та надання можливості пошуку причин невідповідності (якщо такі є) сформованого ФПЗ наперед визначеним цілям або вимогам більш високого рівня, а також надання можливості вдосконалення/уточнення сформованого ФПЗ.

Вимога В3 передбачає несуперечність вимогам/підходам, що викладені у діючих нормативних документах, а також розвиток принципів, що були задекларовані в них.

Для задоволення В4 алгоритм, що має бути покладений у основу метода, має забезпечувати відсутність "тупикових" ситуацій, тобто випадків, в яких виникає неоднозначність трактування результатів (проміжних/остаточних) методу.

Необхідність виконання вимоги В5 полягає у підвищенні якості результатів процесу формування ФПЗ, зокрема несуперечності положенням НД ТЗІ, а також надання ОПР можливості проконтролювати правильність своїх дій.

Вимога В6 висувається з метою підвищення рівня гарантій стосовно процесу розробки ФПЗ та загальної зрілості процесів захисту інформації.

Під В7 необхідно розуміти можливість використання результатів методу для виконання інших робіт зі створення КСЗІ, а також врахування у методі результатів попередніх етапів (наприклад, вимоги політики безпеки та моделі загроз).

Аналіз підстав для ранжирування рівнів послуг (табл. 7) показує, що формально можна виділити 15 таких груп. Проте кожний рівень послуги, залежить передусім від загрози, що блокується чи попереджається. Таке спостереження підтверджується аналізом вимог НД ТЗІ 2.5-004-99:

1. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів.

2. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

3. Рівні починаються з першого (1) і зростають до значення n, де n — унікальне для кожного виду послуг.

Твердження 1. Вибір рівня послуги однозначно зумовлюється загрозою, якій має протистояти КЗЗ чи КСЗІ.

При розробці методу було зроблено спробу представити необхідні дії ОПР у вигляді алгоритму (рис. 1). Проте на практиці це виявилось не

Таблиця 7

Результати аналізу підстав ранжирування функціональних послуг з НД ТЗІ 2.5-004-99

№	Позначення	Підстава ранжирування рівнів послуг
1	КД, КА, КВ, ЦД, ЦА, ЦВ	повнота захисту і вибірковість керування
2	ДЗ, НВ	повнота реалізації
3	КО	-
4	КК	здійснення виявлення, контролю або перекриття прихованих каналів
5	ЦО	множина операцій, для яких забезпечується відкат
6	ДР	повнота захисту і вибірковість керування доступністю послуг КС
7	ДС	спроможність КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови
8	ДВ	міра автоматизації процесу відновлення
9	НР	повнота і вибірковість контролю, складність засобів аналізу даних журналів реєстрації і спроможність вияву потенційних порушень
10	НИ	число задіяних механізмів автентифікації
11	НК	гнучкість надання можливості КЗЗ або користувачу ініціювати захищений обмін
12	НО	вибірковість керування можливостями користувачів і адміністраторів
13	НЦ	міра здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами
14	НТ	можливість виконання тестів у процесі запуску або штатної роботи
15	НА, НП	можливість підтвердження результатів перевірки незалежною третьою стороною

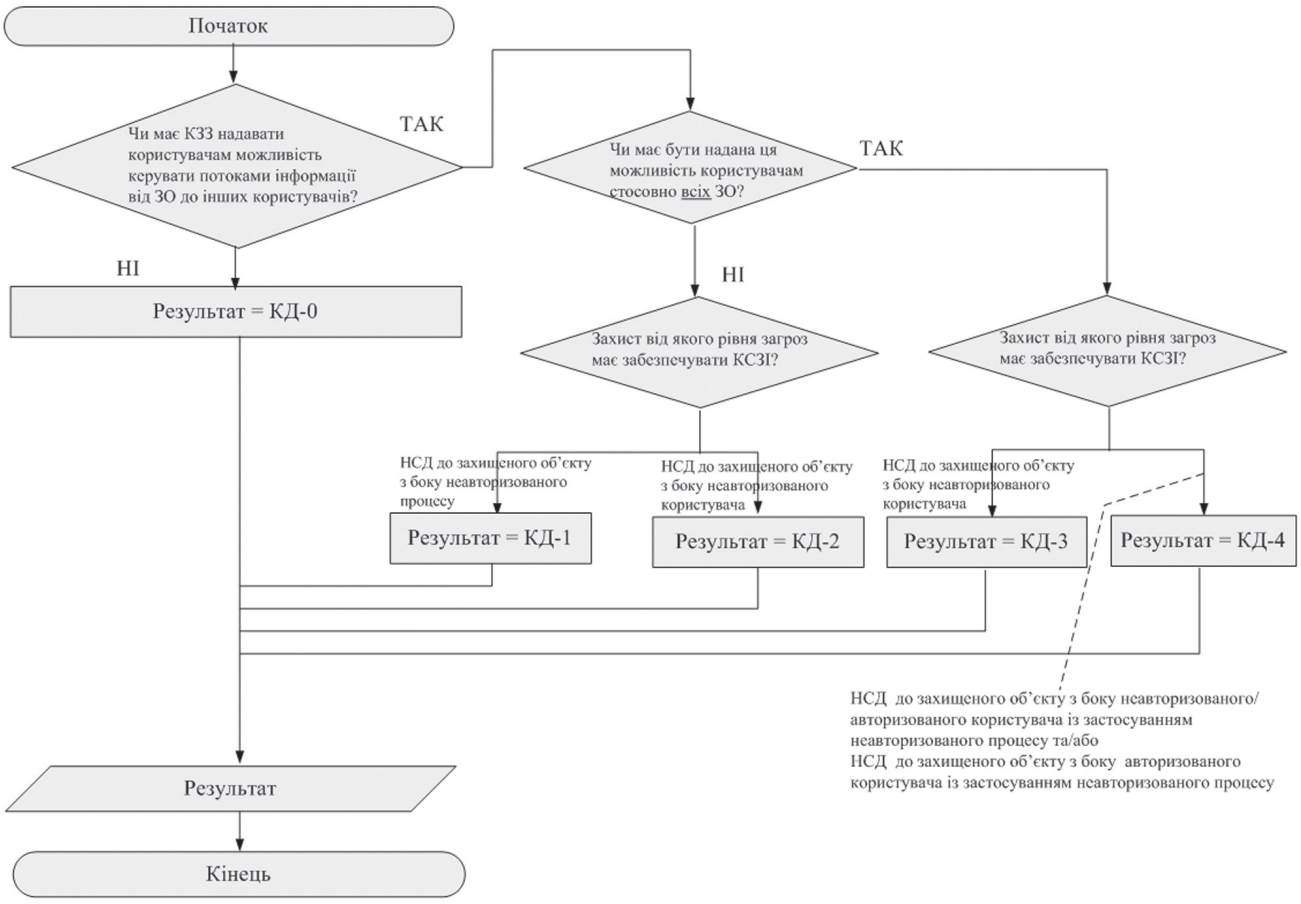


Рис. 1. Алгоритм визначення необхідності включення (та/або рівня) послуги "Довірча конфіденційність"

зручним (вимога В1). Тому алгоритми з'ясування необхідності та рівня послуги безпеки були подані у табличному вигляді (табл. 8).

Таблиця містить 8 основних стовпців: "№", "Запитання", "Відповіді", "Результат", "Перехід до". Стовпець "№" визначає номер кроку експерта по роботі з даною послугою. Стовпець "Запитання" містить формулювання питання закритого типу (тобто такого, що передбачає наявність готових відповідей). Стовпець "Відповіді" розбитий на два підстовпця, в яких по групах наведені варіанти відповідей, з яких має обрати експерт. Стовпець "Результат" також розбито на два підстовпця, в яких наведено зміст отриманого результату, а також його тип "П" (проміжний) чи "О" (остаточний). У останньому стовпці "Перехід до" визначено, до якого кроку слід перейти експерту і яку групу варіантів відповідей він має використовувати при наданні подальших оцінок.

Усього метод містить двадцять дві таких таблиці (за кількістю визначених у НД ТЗІ 2.5-004-99 послуг безпеки). Усі таблиці мають вищеописану структуру (табл. 8) і відрізняються лише наповненням та кількістю кроків (а отже і кількістю рядків), що має пройти експерт.

4.МЕТОД ВЕРИФІКАЦІЇ ПОВНОТИ І НЕСУПЕРЕЧНОСТІ ФПЗ ВІД НСД

Результати дослідження несуперечності стандартних ФПЗ наведені у розділі 2, дозволяють стверджувати, що розробник ФПЗ буде зіткатися із задачею перевіряння розробленого ним ФПЗ.

У загальному випадку розробник ФПЗ може припустити помилки трьох видів:

– не повністю перекрити існуючи загрози;

– не включити до складу ФПЗ залежні (підтримуючі) послуги;

– включити послуги, що не можуть використовуватися спільно.

Для першого виду помилки характерна неможливість її викриття без повторного аналізу загроз, і отже її відсутність пропонується забезпечувати за рахунок запропонованого у статті методу (розділ 3).

Помилки другого та третього виду викриваються достатньо легко за рахунок використання матриць (таблиць) залежностей. Одним із прикладів таких матриць залежностей є морфологічна скринька (рис. 2). У такій таблиці на перетині рядків та стовпців визначається, чи може сумісно використовуватися послуги певних рівнів. Враховуючи те, що основна кількість помилок відноситься до виду "неповнота ФПЗ", у такій морфологічній скриньці слід включити так звані "нульові рівні" послуг. Включення нульового рівня послуги дозволяє у матричному вигляді задати заборону на відсутність послуги у разі використання залежної від неї послуги.

Як видно з рис. 2, користуватися морфологічною скринькою, складеною на основі врахування залежності між функціональними послугами, що визначені у НД ТЗІ 2.5-004-99, незручно унаслідок її надвеликого розміру. До того ж, у разі врахування лише безпосередніх залежностей (як це зроблено у таблицях НД ТЗІ 2.5-004-99) використання морфологічної скриньки може призвести до певних непорозумінь, наприклад, вказано, що рівні

Таблиця 8

Визначення необхідності включення (та/або рівня) послуги "Довірча конфіденційність" табличним способом

№	Запитання	Відповіді		Результат		Перехід до
		Гр.	Варіанти відповіді	Зміст	Тип*	
1	Чи має КЗЗ надавати користувачам (не адміністраторам) можливість керувати потоками інформації від захищених об'єктів КС до інших користувачів?	а)	Так. Ця можливість має бути надана користувачам (не адміністраторам) стосовно окремих захищених об'єктів.	Максимальний рівень послуги: "КД-2"	П	п.2 гр. а)
			Так. Ця можливість має бути надана користувачам (не адміністраторам) стосовно всіх захищених об'єктів.	Мінімальний рівень послуги: "КД-3"	П	п.2 гр. б)
			Ні. КЗЗ має заборонити таку можливість.	У профіль не потрібно включати послугу "КД"	О	
2	Захист від якого рівня загроз має забезпечувати КСЗІ?	а)	НСД до захищеного об'єкту із застосуванням неавторизованого процесу	Рівень послуги: "КД-1"	О	
			НСД до захищеного об'єкту з боку неавторизованого користувача	Рівень послуги: "КД-2"	О	
		б)	НСД до захищеного об'єкту з боку неавторизованого користувача	Рівень послуги: "КД-3"	О	
			НСД до захищеного об'єкту з боку неавторизованого/авторизованого користувача із застосуванням неавторизованого процесу та/або НСД до захищеного об'єкту з боку авторизованого користувача із застосуванням неавторизованого процесу	Рівень послуги: "КД-4"	О	

послуги ДС (ДЗ, ДВ тощо) можуть використовуватися без послуги НИ, але ж це не вірно, оскільки послуга ДС вимагає наявності хоча б першого рівня послуги НО, що в свою чергу тягне за собою щонайменше перший рівень послуги НИ.

Для усунення зазначених недоліків, пропонується розбити морфологічну скриньку на частини. У одній частині (представлена табл. 9) елементом на перетині рядка та стовпця буде визначатися можливість одночасної наявності у ФПЗ послуг з певними рівнями (якщо стоїть "х" одночасно використовувати відповідні рівні послуг у одному ФПЗ заборонено). У другій частині (представлена табл. 10) елементом на перетині рядка та стовпця буде визначатися наявність помилки "неповнота ФПЗ".

Враховуючи те, що велика кількість рівнів послуг ускладнює роботу експерта (розробника), було запропоновано вдосконалений спосіб виявлення помилок типу "неповнота ФПЗ" (таблиці 10 та 11), що має наступні переваги:

– зменшення розмірності таблиці;

– прискорення процесу роботи з таблицями перевірки;

– врахування перехресних посилань (врахування неявної залежності ПОСЛУГА → НО → НИ);

– простота підрахунку послуг, що залежать (обчислення суми по рядкам).

Зменшення розмірності таблиці було досягнуто за рахунок групування рівнів послуг безпеки по групах (11 груп).

Для прискорення процесу роботи з таблицями перевірки було запропоновано використовувати так звані "індекси послуги" (табл. 11). Сутність індексів послуг полягає у наступному: розробник виписує номери, що відповідають рівню послуги (табл. 11) та ставить прапорці у стовпцях з цими порядковими номерами (табл. 10). За рахунок

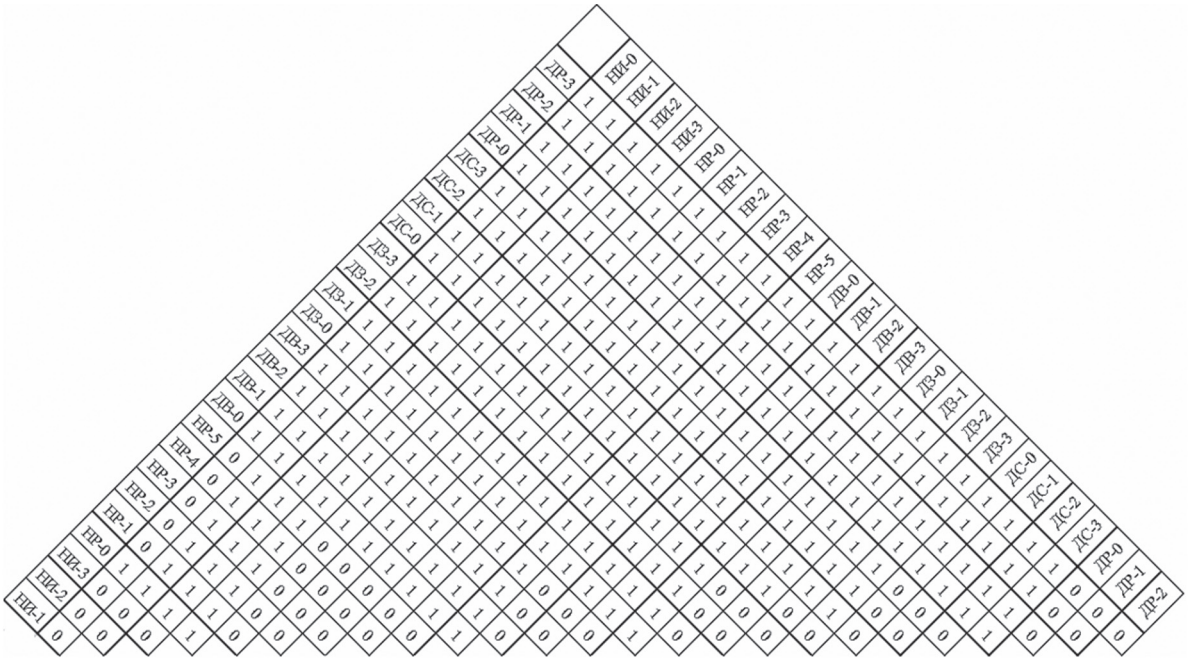


Рис. 2. Фрагмент (26х26) морфологічної скриньки для виявлення помилок типу "неповнота ФПЗ" (реальний розмір повної морфологічної скриньки 89х89)

Таблиця 9

Таблиця перевірки несуперечності послуг з ФПЗ

			Наявність послуги															
			КД-1	КД-2	КД-3	КД-4	КА-1	КА-2	КА-3	КА-4	ЦД-1	ЦД-2	ЦД-3	ЦД-4	ЦА-1	ЦА-2	ЦА-3	ЦА-4
			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Наявність послуги	КД-1	☐							x	x								
	КД-2	☐							x	x								
	КД-3	☐							x	x								
	КД-4	☐							x	x								
	КА-1	☐			x	x												
	КА-2	☐			x	x												
	КА-3	☐			x	x												
	КА-4	☐			x	x												
	ЦД-1	☐															x	x
	ЦД-2	☐															x	x
	ЦД-3	☐															x	x
	ЦД-4	☐															x	x
	ЦА-1	☐											x	x				
	ЦА-2	☐											x	x				
	ЦА-3	☐											x	x				
	ЦА-4	☐											x	x				

Таблиця 10

Виявлення помилок типу “Неповнота ФПЗ”

			Наявність послуги																																			
			КО-1	КВ-1	ЦВ-1	НИ-1	НК-1,2	НЦ-2,3	НВ-1,2,3	КД-1,2	ЦД-1,2	ЦО-1,2	НР-1	НО-1,2,3	НА-1,2	НП-1,2	КА-1,2	КВ-2	ЦА-1,2	ЦВ-2	ДР-1,2, 3	ДС-1,2, 3	ДЗ-1	ДВ-1, 2, 3	НР-2,3,4,5	НТ-1,2, 3	КД-3,4	ЦД-3,4	КА-3,4	ЦА-3,4	КВ-3	ЦВ-3	НЦ-1	КВ-4	ДЗ-2,3	НИ-2,3	КК-1, 3	КК-2	Сума
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
Відсутність послуги	НЦ	☐	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	
	НИ	☐								x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			x	
	КО	☐																									x	x	x	x						x	x	
	НО	☐															x	x	x	x	x	x	x	x	x	x			x	x	x	x	x	x				
	НВ	☐																													x	x		x				
	НР	☐																															x	x				x	
	НК	☐																																		x			
	ДС	☐																																	x			
Код помилки			П0							П1							П2										П3		П4		П5		П6	П7	П8	П9	П10	П11	
Кількість помилок			0																																			

Таблиця 11

Прискорення пошуку за рахунок обчислення індексу послуги

Назва послуги	Позначення послуги	Рівні послуги					Індекс послуги
		1	2	3	4	5	
Довірча конфіденційність	КД	8	8	25	25		
Адміністративна конфіденційність	КА	15	15	27	27		
Повторне використання об'єктів	КО	1					
Аналіз прихованих каналів	КК	35	36	35			
Конфіденційність при обміні	КВ	2	16	30	32		
Довірча цілісність	ЦД	9	9	26	26		
Адміністративна цілісність	ЦА	17	17	28	28		
Відкат	ЦО	10	10				
Цілісність при обміні	ЦВ	3	18	30			
Використання ресурсів	ДР	19	19	19			
Стійкість до відмов	ДС	20	20	20			
Гаряча заміна	ДЗ	21	33	33			
Відновлення після збоїв	ДВ	22	22	22			
Реєстрація	НР	11	23	23	23	23	
Ідентифікація і автентифікація	НІ	4	34	34			
Достовірний канал	НК	5	5				
Розподіл обов'язків	НО	12	12	12			
Цілісність КЗЗ	НЦ	31	6	6			
Самотестування	НТ	24	24	24			
Автентифікація при обміні	НВ	7	7	7			
Автентифікація відправника	НА	13	13				
Автентифікація одержувача	НП	14	14				

того, що ФПЗ за визначенням є: “.. упорядкований перелік рівнів функціональних послуг” (упорядкованість визначається порядком викладення специфікацій послуг у НД ТЗІ 2.5-004-99) перевірка відсутності помилок другого та третього виду для ФПЗ будь-якої складності займає не більше кількох хвилин.

Слід звернути увагу, що при користуванні таблицею 10, прапорець у послугах, що зазначені ліворуч (залежні послуги) позначає, що послуга відсутня у ФПЗ, що верифікується, а прапорці у стовпцях навпаки позначають, що послуга із зазначеним рівнем включена до складу ФПЗ, що верифікується.

Загальний алгоритм роботи експерта з перевіряння несуперечності та повноти ФПЗ може бути викладений у такий спосіб:

– виписати ФПЗ, що верифікується;

– перевірити за табл. 9, чи не присутні в ФПЗ послуги, що не можуть одночасно використовуватися;

– перевірити (з використанням табл. 10 та 11), чи включені до ФПЗ усі залежні послуги;

– у випадку відсутності у ФПЗ, що верифікується, залежних послуг, підрахувати (підсумувавши кількість “x” у рядку) кількість елементів, що зумовили цю помилку;

– підготувати звіт з результатів перевірки.

Розроблений метод верифікації несуперечності та повноти ФПЗ від НСД може використовуватися як для перевірки ФПЗ, що розроблені за методом, викладеним у розділі 3, так і для перевірки будь-якого іншого ФПЗ, що розроблений згідно вимог, що висуваються НД ТЗІ 2.5-004-99 [2].

ВИСНОВКИ

1. Нормативне та методичне забезпечення з організації діяльності із запобігання загрозам НСД відстає від світового рівня. Наявні нормативні документи, зокрема, не надають методів формування та перевіряння ФПЗ.

2. Існуючий підхід, заснований на стандартних ФПЗ, призводе до висунення недостатніх або надмірних вимог до захисту КС.

3. Запропоновані методи дозволяють підвищити ефективність діяльності експерта з розробки та верифікації ФПЗ за рахунок:

– зручності використання;

– зрозумілості проміжних результатів;

– можливості самоперевірки;

– забезпечення повторюваності та порівнюваності результатів;

– врахування результатів інших етапів побудови КСЗІ.

Література.

[1] НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від "28" квітня 1999 р. / ТОВ "ІКТ". – К: ДСТСЗІ СБ України, 1999. – 21 с. – (Нормативний документ системи технічного захисту інформації).

[2] НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від "28" квітня 1999 р. / ТОВ "ІКТ". – К: ДСТСЗІ СБ України, 1999. – 59 с. – (Нормативний документ системи технічного захисту інформації).

[3] НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від " 28 " квітня 1999 р. /ТОВ "ІКТ2. – К: ДСТСЗІ СБ України, 1999. – 22 с. – (Нормативний документ системи технічного захисту інформації).

[4] *Лєншин А.В., Буслов П.В.* Метод формування функціональних профілів захищеності від несанкціонованого доступу //Науково-технічний журнал "Радіоелектронні і комп'ютерні системи". – Харків: ХАІ, 2010. – Том 7. – С. 77-81

Надійшла до редколегії 9.07.2010.

Потій Олександр Володимирович, доцент, доктор техн. наук, професор кафедри БІТ ХНУРЕ. Область наукових інтересів: системний аналіз процесів захисту інформації, управління захистом інформації.

Лєншин Анатолій Валерійович, канд. техн. наук, доцент кафедри БІТ ХНУРЕ. Область наукових інтересів: побудова КСЗІ, інфраструктура відкритих ключів.

УДК 681.3.06

Методы построения и верификации непротиворечивости и полноты функциональных профилей защищенности от несанкционированного доступа / А.В.Потий, А.В Леншин // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 479–488.

Проведен анализ требований нормативных документов в части формирования профилей защищенности. Определены недостатки существующего подхода к формированию профиля защищенности. Сформулированы требования к методу формирования и методу проверки непротиворечивости и полноты профилей защищенности, дано их описание. Показано, что разработанные методы соответствуют требованиям по: временной сложности, стандартизированности подхода (повторяемость и сравнимость результатов), непротиворечивости требованиям нормативных документов, понятности промежуточных результатов и их воздействий на окончательный выбор, а также возможности самопроверки лица, использующего метод.

Ключевые слова: профиль защищенности, несанкционированный доступ, методы системного анализа.

Табл. 11. Ил.02. Библиогр.: 04 назв.

UDC 681.3.06

Methods of constructing and verifying consistency and completeness of functional protection profiles against unauthorized access / A V. Potii, A.V. Lenshin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 479-488.

The analysis of normative documents requirements concerning protection profiles is conducted. Shortcomings of the existing approach to designing protection profiles are identified. Requirements to the methods of designing and verifying consistency and completeness of protection profiles against unauthorized access are formulated and their descriptions are given. It is shown that the developed methods comply with the requirements of time complexity, approach standardization (repeatability and comparability of results), consistency to the requirements of the normative documents, understandability of interim results and their impact on the final choice, as well as the possibility of self-verification for a person using the method.

Key words: protection profile, unauthorized access, system analysis methods.

Tab. 11. Fig. 02. Ref.: 04 items.

УДК 519.688

ОСОБЛИВОСТІ ЕЦП З ВІДНОВЛЕННЯМ ПОВІДОМЛЕННЯ

О. А. ШЕВЧУК

Досліджуються відмінності підписів з відновленням повідомлення з підписами з додатком. Робляться зауваження щодо використання підписів з відновленням повідомлення. Шляхом декомпозиції показується структурова схожість підписів з відновленням та доповненням.

Ключові слова: ЕЦП, доповнення повідомлення, відновлення повідомлення.

ВСТУП

У найближчі роки Україна планує завершити гармонізацію підписів з відновленням повідомлення. Ці схеми ЕЦП на відміну від загальновживаних підписів з додатком мають особливості. У специфічних ситуаціях ці особливості можуть зробити використання ЕЦП виправданим, коли впровадження звичайного підпису з додатком може бути неефективним, або неможливим.

Ефективному впровадженню підписів з відновленням повідомленням заважає обмеженість інформації щодо їх спеціальних властивостей, їх порівняння та визначення відповідної до кожного підпису галузі застосування.

Метою статті є огляд деяких властивостей схем ЕЦП з відновленням міжнародного стандарту ISO/IEC 9796-3.

Для досягнення цієї мети необхідно сформувати абстрактну модель підпису, визначити властивості підписів з відновленням, у тому рахунку і ті, що не мають прямого відношення до надання послуг безпеки інформації, порівняти ЕЦП з відновленням повідомлення та ЕЦП з доповненням.

1. ДЕКОМПОЗИЦІЯ ЕЦП

Стандарти ISO/IEC мають схематичні позначення процесів формування/перевірки ЕЦП, але для задач порівняння властивостей вони є дещо збитковими та не наочними. На початкових етапах можна знехтувати такими елементами схем: виробленням доменних параметрів (у зв'язку з еквівалентністю алгоритму в усіх схемах ЕЦП з доповненням у стандарті з однаковим математичним апаратом), функціями морфізмів даних між різними категоріями (морфізм точки до цілого тощо). Ці функції є технічними, хоча від їх адекватності залежить загальна безпека усієї схеми, але у межах стандарту функції морфізмів вживаються однаково та однакові, тому на переваги схеми відносно стандарту не впливають.

Першу наочну властивість ЕЦП з відновленням повідомлення отримаємо за допомогою структурової декомпозиції та порівняння загальної схеми з відновленням повідомлення Ніберг-Рюпеля, та схеми з доповненням повідомлення. Для схеми ЕЦП з доповненням повідомлення можливо попередньо зробити таку декомпозицію (у дужках еквівалентні компоненти схеми ECDSA):

1. Вироблення доменних параметрів
2. Вироблення особистого ключа $d \in [1, n-1]$
3. Обчислення відкритого ключа $Q = d \times G$
4. Вироблення передпідпису Π: $k \in [1, n-1]$ $\Pi = k \times G$
5. Обчислення ідентифікатору повідомлення $i = Hash(M)$
6. Формування зворотньої компоненти підпису $\pi((x, y)) = x$; $r = \pi(\Pi)$
7. Обчислення незворотньої компоненти підпису (s-компоненти) $s = k^{-1}(i + dr)$
8. Формування пакету ЕЦП зі зворотньою та незворотньою компонентами та тілом повідомлення (r, s, M)
9. Передача пакету $sizeof(r, s, M)$
10. Відновлення передпідпису з переданої незворотньої компоненти за допомогою ідентифікатору повідомлення та зворотньої компоненти, що було передано у складі підпису $i = Hash(M)$; $\Pi = iw \times G + rw \times G$
11. Обчислення зворотньої компоненти з передпідпису $r' = \pi(\Pi)$
12. Прийняття рішення щодо дійсності підпису, виходячи з еквівалентності обчисленої та переданої відновлюваної частини підпису. (Якщо $r' = r$ підпис вірний)

Відповідно, схеми ЕЦП з відновленням повідомлення мають мати такі компоненти (у дужках еквівалентні компоненти схеми ECNR).

1. Вироблення доменних параметрів
2. Вироблення особистого ключа $d \in [1, n-1]$
3. Обчислення відкритого ключа $Q = d \times G$
4. Вироблення передпідпису $\Pi = kG$
5. Доповнення повідомлення

$$M = M_{rec} \| M_{clr}$$
$$L(M_{rec}) \le L_{max}$$
$$pad = I2OSP(1, L_{max} + 1 - L(M_{rec}))$$
$$\tilde{M}_{rec} = pad \| M_{rec}$$
$$h = Hash_1(\tilde{M}_{rec})$$
$$d = h \| (Hash_2(h) \oplus \tilde{M}_{rec}),$$

де h – геш токен, а pad – доповнення

6. Формування зворотньої компоненти підпису шляхом маскування доповненого повідомлення з передпідписом $r = (\delta + \pi(\Pi)) \bmod n$
7. Обчислення незворотньої компоненти підпису $s = (k - dr) \bmod n$

8. Формування пакету ЕЦП зі зворотньої та незворотньої компонент та відкритої частини повідомлення (r, s, M_{clr})

9. Передача пакету $sizeof(r, s, M_{clr})$

10. Відновлення передпідпису з переданої незворотньої компоненти за допомогою ідентифікатору повідомлення та зворотньої компоненти, що було передано у складі підпису $\Pi = sP + rQ$

11. Обчислення доповненого повідомлення шляхом зворотнього маскування зворотньої компоненти підпису з передпідписом $\delta = (r - \pi(\Pi)) \bmod n$

12. Висновок щодо дійсності підпису, виходячи з семантики доповненого повідомлення. Якщо h має сенс, згідно до m – підпис дійсний.

Таким чином, можна навести структурну різницю між зазначеними типами підписів: схеми з відновленням не мають механізмів чіткої перевірки дійсності повідомлення (кроки (12), (12) відповідно). Якщо підпис з додатком представити як повідомлення $(r, s) \| M$, а процес перевірки – як перевірку семантичного змісту повідомлення $[(r, s) \| M]$, тоді розбіжності буде усунено. Дійсно, відірваний від повідомлення підпис (r, s) є не більш, ніж кортежем, що не має ніякого семантичного змісту.

Процесс формування пакету підпису у цих ЕЦП також є дещо іншим. Схеми з відновленням не обов'язково мають мати тіло повідомлення у складі пакету підпису (кроки (8)-(8) відповідно) – ситуація, коли частина повідомлення, або все, включається до r компоненти є штатною.

Таким чином, ЕЦП з відновленням повідомлення семантично відповідають схемам з додатком. Завдяки зазначеним розбіжностям, схеми з відновленням мають особливості: зменшення розміру підпису (за рахунок маскування у зворотній компоненті), та деякі додаткові властивості. Зменшення підпису має негативні наслідки – підпис може мати менший розмір за рахунок зменшення збитковості, але це робить його потенційно більш вразливим до екзистенційної підробки.

Доцільно досліджувати такі властивості підписів з відновленням повідомлення:

– стійкість до атаки екзистенційної та селективної підробки у залежності від кількості інформації, що вкладено до компоненти ЕЦП, що відновлюється

– часові показники

– можливість надання послуги конфіденційності та особливості

– складність вироблення підпису.

У наступній частині будуть зроблені базові дослідження за сформульованим напрямком підписів стандарту ISO/IEC 9796-3 – ECNR, ECPV, ECAO, ECMR, ECKNR.

2. ЕКЗИСТЕНЦІЙНА ТА СЕЛЕКТИВНА ПІДРОБКА, ДОДАТКОВІ ВЛАСТИВОСТІ

Як було відмічено, основним питанням до схем ЕЦП з відновленням повідомлення є визначення стійкості до екзистенційної та селективної підробки. У загальному вигляді остаточне прийняття рішення про дійсність повідомлення робиться через визначення дійсності збитковості відносно повідомлення. Таким чином, задача екзистенційної підробки зводиться до формування $n^{n/2}$ повідомлень δ_i, де n-бітовий обсяг збитковості повідомлення δ. Можливо казати про успішність атаки, коли для повідомлення δ' буде знайдене повідомлення δ'' таке, що усі n біт збитковості для повідомлень δ' та δ'' будуть еквівалентними.

Потрібно відрізняти вірогідність підробки для включеного в підпис повідомлення, та частини, що передається у відкритому вигляді.

Селективна підробка для підписів з відновленням повідомлення у загальному випадку має однаковий семантичний зміст з повним розкриттям, тому що частина повідомлення приймає безпосередню участь в обчисленні підпису.

Алгоритми з відновленням повідомлення також не мають рекомендацій відносно кількості біт надлишковості. Тому визначимо граничні показники відносно надлишковості.

Розглянемо особливості схем підписів.

Схема ECMR допускає можливість для багатопотокової оптимізації на етапі перевірки підпису. Один з етапів (обчислення R'):

$$R' = ((1 + OS2IP(r) + s)/OS2IP(r)) \times P + \\ + (s/OS2IP(r)) \times Q;$$

Таблиця 1

Показники підписів

	ECNR	ECAO	ECPV	ECMR	ECKNR
Мінімальний бітовий обсяг зворотньої компоненти	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$	2	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$
Максимальний бітовий обсяг зворотньої компоненти	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$	∞	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$
Максимальний бітовий обсяг повідомлення δ	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$	∞	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$
Максимальний бітовий обсяг збитковості	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$	∞	$\lceil \log_2 n \rceil$	$\lceil \log_2 n \rceil$
Максимальний бітовий обсяг збитковості у залежності від обсягу повідомлення M	$\lceil \log_2 f \rceil$ - $\lceil \log_2 M \rceil$	$\lceil \log_2 f \rceil$ - $\lceil \log_2 M \rceil$	∞	$\lceil \log_2 f \rceil$ - $\lceil \log_2 M \rceil$	$\lceil \log_2 f \rceil$ - $\lceil \log_2 M \rceil$

Можна побачити, що компоненти

$$((1+OS2IP(r)+s)/OS2IP(r))\times P$$

$$\text{та } (s/OS2IP(r))\times Q$$

можуть бути обчислені паралельно після обчислення $(OS2IP(r))^{-1} \bmod n$.

Схема ECAO має додаткову властивість – гарантоване використання природної збитковості. Функція ділить повідомлення на частину, що включена до підпису (M_{rec}), та частину, що передається відкритою (M_{clr}). Частина M_{rec} подвійно гешується: перший геш використовується у незмінному вигляді, друга частина використовується як збитковість для першої, та додається до підпису.

$$M = M_{rec} \| M_{clr}$$
$$L(M_{rec}) \le L_{max}$$
$$pad = I2OSP(1, L_{max} + 1 - L(M_{rec}))$$
$$\tilde{M}_{rec} = pad \| M_{rec}$$
$$h = Hash_1(\tilde{M}_{rec})$$
$$d = h \| (Hash_2(h) \oplus \tilde{M}_{rec})$$

Схема ECPV представляє свою функцію маскування та формування зворотньої компоненти підпису, у якої зворотня компонента формується шляхом підстановки за ключем, що сформовано за функцією розгортання ключів з передпідпису.

Таким чином, максимальна складність атаки екзистенційної підробки для ECAO та ECNR складе $2^{n/2}$, а для ECPV – довільна. Визначимо мінімально необхідний бітовий обсяг наданої збитковості для забезпечення безпечного часу з вірогідністю 0.95 на протязі року, якщо криптоаналітик може обчислювати 10^8 збитковостей за секунду. Для цього випадку

$$n = \lceil log_2(\frac{\gamma tk}{P}) \rceil = \lceil log_2(\frac{10^8 * 1 * 3{,}15 * 10^7}{0{,}95}) \rceil = 52 .$$

Схема ECKNR відрізняється від ECNR додатковим кроком при формуванні r компоненти підпису: за передпідписом формується гамма, до якої додається гамма сформована за участю відкритої частини повідомлення. Таким чином, може бути досягнута деяка гнучкість при формуванні повідомлення зі збитковістю d.

3. НАДАННЯ ПОСЛУГИ КОНФІДЕНЦІЙНОСТІ

Схеми ЕЦП з відновленням повідомлення «приховують» частину повідомлення по суті у цифровому підписі.

В усіх схемах зворотня частина повідомлення сформована шляхом маскування повідомлення з передпідписом. У загальному вигляді перетворення можна представити у вигляді $c = Mask(Msg, KDF(kG))$.

Відновити повідомлення можливо у разі відтворення передпідпису kG, що у загальному випадку можливо тільки при перевірці ЕЦП. Таким чином, можна стверджувати, що повідомлення може відновити лише за наявності відкритого ключа. У відкритих системах така схема не має сенсу з надання послуг конфіденційності, але у разі, якщо циркуляція відкритих ключів в системі є контрольованою, є сенс у використанні цієї властивості схем з доповненням.

ВИСНОВКИ

Схеми з доповненням повідомлення мають усі властивості ЕЦП з відновленням повідомлення. Обмежене надання послуги конфіденційності можливе у закритих системах, де можна реалізувати контрольований процес поширення відкритого ключа.

ЕЦП з відновленням може мати більший бітовий обсяг повідомлення. Але при цьому істотно збільшується ймовірність екзистенційної підробки (в усякому разі ймовірність екзистенційної підробки підпису з відновленням повідомлення значно вижче, ніж у підпису з доповненням).

Основними характеристиками, що є особливими для підпису з відновленням повідомлення, є:

– ймовірність екзистенційної підробки у залежності від довжини модуля обчислень та повідомлення, що передається,

– ймовірність екзистенційної підробки у залежності від довжини модуля обчислень та повідомлення, що відновлюється,

– ефективність використання природньої збитковості повідомлення,

– можливість розпаралелювання, максимальний та мінімальний обсяг пакету підпису,

– варіативність обсягу пакету підпису.

Кожен з підписів з відновленням повідомлення стандарту ISO/IEC 9796-3 має особливості. Доцільно обирати більш раціональний підпис у залежності від ситуації. Наприклад:

– ECNR доцільно застосовувати для незбиткових повідомлень та не більше обраного модуля перетворень, але і не значно меньшого, наприклад, команд RPC,

– ECAO для збиткових повідомлень,

– ECPV для повідомлень з нефіксованою довжиною повідомлення, або надкоротких повідомлень, наприклад, команд контроллеру,

– ECKNR для великих повідомлень із захищеним заголовком, можливо для IP пакетів.

Литература.

[1] *Мао Венбо.* Современная криптография: Теория и практика / Венбо Мао; Ред. Тригуб С. Н. – 03150, Киев, а/я 152: Издательский дом Вильямс, 2005.

[2] *Горбенко И.Д.* Защита информации в информационно-телекоммуникационных системах. Ч.1. Криптографическая защита инфомации / И.Д. Горбенко, Т.О. Гриненко. – ХНУРЭ, 2004.

[3] ISO/IEC 9796-3: Discrete logarithm based mechanisms / ISO/IEC. – URL:http://www.iso.org/, 2006.

[4] Nyberg K., Rueppel R. A new signature scheme based on the dsa giving message recovery / Rueppel R. Nyberg K. // ACM Conference on Computer and Communications Security. P. 58–61.

Надійшла до редколегії 8.07.2010.

Шевчук Олексій Анатолійович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: захист інформації в інформаційно-телекомунікаційних системах, ЕЦП з відновленням повідомлення.

УДК 519.688

Особенности ЭЦП с восстановлением сообщения / А. А. Шевчук // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 489–492.

Исследуются различия подписей с восстановлением сообщения. Вырабатываются замечания к использованию подписей с восстановлением сообщения. Путем декомпозиции показывается структурная схожесть подписей с восстановлением и дополнением.

Ключевые слова: ЭЦП, восстановление сообщения, дополнение сообщения.

Табл. 01. Библиогр.: 04 назв.

UDC 519.688

Particulars of digital signatures with message recovery / O.A. Shevchuk // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 489-492.

Differences between signatures with message recovery are investigated. Remarks relating to the use of signatures with message recovery are made. Structural similarity of recovery and addition signatures is shown by means of decomposition.

Key words: digital signature, message recovery, message addition.

Tab. 01. Ref.: 04 items.

К 75-ЛЕТИЮ со дня рождения Академика Академии наук прикладной радиоэлектроники, лауреата Государственной премии СССР, Заслуженного изобретателя УССР, доктора технических наук, профессора ГОМОЗОВА ВЛАДИМИРА ИВАНОВИЧА

8 июня 2010 года исполнилось 75 лет со дня рождения Академика Академии наук прикладной радиоэлектроники, лауреата Государственной премии СССР, Заслуженного изобретателя УССР, доктора технических наук, профессора, полковника в отставке Гомозова Владимира Ивановича.

Владимир Иванович Гомозов родился в г. Москве. В 1953 г., после окончания с золотой медалью средней школы, поступил и в 1958 г. закончил Артиллерийскую радиотехническую академию Советской Армии им. Маршала Советского Союза Говорова Л.А. (г. Харьков) по радиотехнической специальности с присвоением квалификации военного инженера по радиолокации. Доктор технических наук с 1983 г. (кандидат технических наук с 1966 г.), профессор с 1984 г. (доцент с 1973 г.), лауреат Государственной премии СССР в области радиолокации (1979 г.), Заслуженный изобретатель УССР (1976 г.). Награжден орденом «За службу Родине в Вооруженных Силах СССР III степени» (1984 г.) и двенадцатью медалями СССР, Грамотой Верховного Совета СССР «Воину-интернационалисту», медалью «За содружество в борьбе с агрессорами» и грамотой Президиума Народного собрания ДРВ (Вьетнам, 1973 г.).

С 1953 г. по 1992 г. – служба в Вооруженных Силах СССР на различных должностях: начальник радиолокационной станции, инженер дивизии радиотехнических войск ПВО (1958-1960 г.г.); инженер, младший научный сотрудник Проблемной научно-исследовательской лаборатории (1961-1965 г.г.) и преподаватель (1966-1972 г.г.) Артиллерийской радиотехнической академии С.А. им. Говорова Л.А.; специалист-советник ограниченного контингента Советских войск во Вьетнаме (1973 г.); старший научный сотрудник, преподаватель, старший преподаватель и начальник кафедры тактики и вооружения ПРО (1974-1992 г.г.) Военной инженерной радиотехнической академии ПВО им. Говорова Л.А.

С 1992 г. работает в Открытом Акционерном Обществе «АО Научно-исследовательский институт радиотехнических измерений» Национального Космического Агентства Украины на должностях: начальника отделения — главного конструктора направления по радиотехническим средствам радиолокации, радиоэлектронного подавления и наземных автоматических комплексов управления космическими аппаратами; заместителя директора по подготовке научных кадров, главного научного сотрудника. Много лет руководил специализированным ученым советом по защите докторских (кандидатских) диссертаций при ОАО «АО НИИРИ». Подготовка высококвалифицированных специалистов и научных кадров является для В.И.Гомозова одной из приоритетных задач. В течение многих лет он являлся председателем Государственной экзаменационной комиссии на радиотехническом факультете Харьковского Национального университета радиоэлектроники.

Область научных интересов В.И.Гомозова охватывает широчайший круг проблем: теория и техника генерирования, модуляции, стабилизации, измерения параметров сложных СВЧ сигналов и фокусировки электромагнитного поля в однопозиционных и многопозиционных излучающих структурах радиотехнических систем (радиосвязи, радионавигации, радиолокации и радиотелеуправления летательными аппаратами). Автор или соавтор 316 опубликованных научно-технических работ (без учета отчетов по НИР и ОКР): 31 научно-методического труда в том числе, шесть учебников по теории и технике генерирования, излучения и приема радиолокационных сигналов, построению и эксплуатации радиоэлектронного вооружения и шесть монографий по теории автоколебаний и формированию сложных сигналов радиоэлектронных систем (1990-2010 г.г.); 149 научно-технических статей в академических и ведомственных журналах (1959-2010 г.г.); 140 изобретений, защищенных авторскими свидетельствами СССР, патентами России и Украины (1964-1997 г.г.).

Впервые в мировой практике на три года раньше, чем в США, В.И.Гомозов при научном руководстве Н.Д.Колпакова разработал на ЛОВ типа М однокаскадный передатчик ЛЧМ сигналов сантиметрового диапазона волн, мощностью 100 КВт, длительностью импульса 2 мкс и девиацией частоты 72 МГц (1962 г.) и, будучи ответственным исполнителем в группе экспериментаторов, под научным руководством Я.Д.Ширмана на созданной экспериментальной РЛС подтвердил в натурных условиях, что при использовании техники формирования и сжатия ЛЧМ сигналов можно получить разрешение по дальности 3-3,5 м. Результаты развития этих работ и разработанные затем унифицированные аналогово-цифровые формирователи зондирующих и гетеродинных сложных сигналов использованы при создании четырех принципиально новых промышленных образцов радиолокационного вооружения (1968-1992 г.г.).

Важным научным направлением исследований В.И. Гомозова является динамическая теория угловой модуляции и автоподстройки частоты (фазы) автоколебаний. Этими работами проф. Гомозов В.И. начал заниматься в 1962 г.

В результате была развита теория автоколебаний и флуктуации их частоты (фазы) и были получены новые нелинейные дифференциальные однородное и неоднородное управления автоколебаний, а также стохастическое нелинейное дифференциальное неоднородное уравнение для флуктуаций частоты автоколебаний, на основе которых более адекватно наблюдаемым экспериментально процессам отражаются баланс фаз, характер установления, величины выбегов и стационарные значения частоты, причины и уровни флуктуаций частоты, чем на основе считавшихся с 1922 г. классических уравнений Ван-дер-Поля (1980-1991 г.г.).

В рамках указанных научных направлений и интересов проф. В.И.Гомозова им созданы пять научных школ и подготовлено 45 кандидатов технических наук, 6 докторов технических наук и профессоров. Среди учеников — лауреат Премии Правительства России, Заслуженный изобретатель России, Заслуженный изобретатель Украины, Почетный работник высшего профессионального образования Российской федерации.

Признанием научной общественностью фундаментальных и прикладных исследований В.И.Гомозова явилось назначение ему стипендии Президента Украины для выдающихся ученых с июля 2007 г.

Вместе со всей научной общественностью сердечно поздравляем Владимира Ивановича с 75-летием и от всей души желаем юбиляру крепкого здоровья, неиссякаемой энергии, оптимизма, творческих успехов и больших свершений во славу науки.

ПРИКЛАДНАЯ РАДИОЭЛЕКТРОНИКА

Научно-технический журнал

Ответственный секретарь

Е. Б. Исаева

Корректор

А. И. Шахова

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 30.09.2010 р.).

Рекомендовано Вченою радою Харківського національного університету радіоелектроніки
(протокол № 64 від 04.10.2010 р.).

Свідоцтво про державну реєстрацію КВ № 6037 від 09.04.2002 р.

Підписано до друку 04.10.2010. Формат 60 × 84 $^{1}/_{8}$.
Папір офсет. Друк офсет. Умов.-друк. арк. 21,6. Облік.-вид. арк. 22,0.
Тираж 300 прим. Ціна договірна.

Надруковано ФОП Андреєв К.В.
61166, м. Харків, просп. Леніна, 14. Тел. 757-63-27