УДК 621.391

Евсеев С.П., Король О.Г.

АНАЛИЗ МЕТОДОВ ПОСТРОЕНИЯ УНИВЕРСАЛЬНЫХ КЛАССОВ ХЕШ-ФУНКЦИЙ

Постановка проблемы в общем виде и анализ литературы

Для обеспечения аутентичности используются процедуры традиционного и асимметричного шифрования, функции хеширования, а также коды аутентичности (MAC-коды) [1, 13]. Проведенный анализ показал [1, 12, 13], что MAC-коды (UMAC-16, UMAC-32) – криптографические примитивы фиксированной длины (16 и 32 бита соответственно), основанные на универсальных классах хеш-функций обладают самыми высокими показателями скорости хеширования (10^9 бит/с). При их формировании используются трехслойные схемы UHash16 и UHash32, основанные на семействах универсальных хеш-функций [1, 12, 13].

Целью данной статьи является анализ процедур универсального хеширования к конструированию безусловно стойких аутентификационных кодов без секретности, рассмотрение формальных определений некоторых семейств универсальных хеш-функций для их применения при конструировании кодов аутентификации (UMAC-16, UMAC-32).

1. Общие понятия универсальных классов

Универсальные классы хеш-функций были впервые предложены Картером и Вегманом [2], далее изучены Сарвате [4] и Стинсоном [6 – 10]. Рассмотрим основные определения для описания универсальных классов.

Пусть A и B будут конечными множествами из соответствующих элементов $a = |A|$ и $b = |B|$, где $a \geq b$. Функция $h: A \rightarrow B$ будет названа *хеш-функцией*. Для хеш-функции h и для $x, y \in A$, $x \neq y$, определим $\delta_h(x, y) = 1$, если $h(x) = h(y)$ и $\delta_h(x, y) = 0$ в обратном случае. То есть, $\delta_h(x, y) = 1$ тогда и только тогда, если хешированные значения x и y вызывают коллизию. Для конечного множества H хеш-функций определим $\delta_{H(x,y)} = \sum_{h \in H} \delta_{h(x,y)}$. Отсюда $\delta_H(x,y)$ подсчитывает количество хеш-функций в H, при которых значения элементов x и y вызывают коллизию.

Идея универсального класса хеш-функций заключается в определении набора элементов конечного множества H хеш-функций таким образом, что случайный выбор функции $h \in H$ обеспечивал бы низкую вероятность того, что для любых различных входов x и y, вероятность того, что $h(x) = h(y)$ (вероятность коллизии) не может быть больше ε: $P_{кол} = P(h(x) = h(y)) \leq \varepsilon$, и может быть подсчитана как $\delta_H(x, y)/|H|$.

Определение универсального класса хеш-функций эквивалентно определению такого алгоритма формирования кода аутентификации, при котором выполняется следующее условие: число различных правил формирования кода аутентификации (число ключей), при которых существует коллизия (совпадение кодов аутентификации) для двух произвольных входных последовательностей, ограничено. Число таких ключей не может превосходить значение $P_{кол} \cdot H$, где $P_{кол}$ – вероятность коллизии, H – число всех правил (ключей).

Теорема 1. [4] Для любого класса H хеш-функций от A к B существуют различные элементы $x, y \in A$, такие что $\delta_H(x,y) \geq |H|(a - b)/(b(a - 1))$, где $a = |A|$ и $b = |B|$.

Приведем два определения классов хеш-функций.

1. Пусть $0 < \varepsilon < 1$. H является ε - *универсальным хеш-классом (сокращенно* $\varepsilon - U(H,a,b)$*)*, если для двух различных элементов $x_1, x_2 \in X$ существует не больше чем $H \cdot \varepsilon$ функций $f \in H$ таких, что $h(x) = h(y)$, если $\delta_H(x, y) \leq \varepsilon|H|$ для всех $x, y \in A$, $x \neq y$.

2. Пусть $0<\varepsilon<1$. H является *ε-строго универсальным хеш-классом* (сокращенно $\varepsilon-SU(H,a,b)$) если выполняются следующие условия: 1.Для каждого $x_1 \in A$ и для каждого $y_1 \in B$,

$$\left|\{h \in H : h(x_1) = y_1\}\right| = |H|/|B|$$

2. Для каждого $x_1, x_2 \in A$ $(x_1 \neq x_2)$ и для каждого $y_1, y_2 \in B$,

$$\left|\{h \in H : h(x_1) = y_1, h(x_2) = y_2\}\right| \leq \varepsilon|H|$$

Определение строго универсального класса хеш-функций эквивалентно определению алгоритма формирования кодов аутентификации. Используя строго универсальный класс хеш-функций можно построить схему аутентификации, при котором, будут выполняться следующие правила:

1. Число правил формирования кода аутентификации (число ключей), при которых для произвольной входной последовательности значение кода аутентификации не изменяется, ограничено. Число таких ключей не может превосходить значения $\frac{H}{2^a}$, где H - число всех ключей, a - число бит кода аутентификации;

2. Число правил формирования кода аутентификации (число ключей), при которых для двух произвольных входных последовательностей соответствующие им значения кода аутентификации не изменяются, ограничено. Число таких ключей не может превосходить значения $P_{кол} \cdot \frac{H}{2^a}$, где $P_{кол}$ – вероятность коллизии, H – число всех ключей, a – число бит кода аутентификации.

Вероятность коллизии кодов аутентификации в такой схеме будет определяется следующим утверждением $P_{кол} \leq \varepsilon$.

2. Нижние границы на размер классов хеш-функций

С точки зрения того факта, что классы хеш-функций приводят к аутентификационных кодам, есть интерес посчитать нижние границы числа требуемых хеш-функций. Рассмотрим некоторые ранее известные границы.

Теорема 2 [9]. Если существует $\varepsilon-SU(H,a,b)$ класс H хеш-функций от A до B, где a = |A| и b= |B|, тогда

$$\left|H \geq \frac{a(b-1)}{a(\varepsilon b-1)+b^2(1-\varepsilon)}\right|.$$

Подставив $\varepsilon = 1/b$ и $\varepsilon = (a–b)/(ab –b)$ в приведенную выше границу, соответственно получим следствие.

Следствие 1 [9]. Предположим, H это класс хеш-функций от A до B, где a = |A| и b = |B|. Если H является $\varepsilon-U(H,a,b)$, тогда $|H| \geq a/b$. Если H есть $\varepsilon-SU(H,a,b)$, тогда $|H| \geq (a-1)/(b-1)$.

Далее представим нижнюю границу на число хеш-функций в $\varepsilon-U(H,a,b)$ – классе.

Теорема 3 [9]. Если существует $\varepsilon-U(H,a,b)$ класс H хеш-функций от A до B, где a = |A| и b = |B|, тогда

$$\left|H \geq 1+\frac{a(b-1)^2}{b\varepsilon(a-1)+b-a}\right|$$

В случае $\varepsilon = 1/b$ получаем следующее следствие.

Следствие 2 [9]. Если существует $\varepsilon-SU(H,a,b)$ класс H хеш-функций от A до B, где a = |A| и b = |B|, тогда $|H| \geq 1 + a(b-1)$. Если $|H| = 1 + a(b-1)$ тогда существует OA (b, a, λ), где $\lambda = (a(b-1)+1)/a^2$ (OA(b, a, λ) – ортогональный массив).

3. Прямые и рекурсивные конструкции для построения универсальных классов хеш функций

Рассмотрим некоторые прямые и рекурсивные конструкции для универсальных классов хеш-функций из [2, 9].

Теорема 4 [2, 9] . Пусть q будет степенью простого числа. Тогда существует $\varepsilon - U(H,a,b)$ класс H хеш-функций от A до B, где $|A| = q^2$, $|B| = q$ и $|H| = q$ (отсюда $\varepsilon = 1/q$).

Доказательство. Пусть $A = GF(q) \times GF(q)$, $B = GF(q)$ и $H = \{h_x : x \in GF(q)\}$, где $h_x(a,b) = b - ax$.

Теорема 5 [2, 9]. Пусть q будет степенью простого числа. Тогда существует $\varepsilon - SU(H,a,b)$ класс H хеш-функций от A до B, где $|A| = q^2$, $|B| = q$ и $|H| = q^3$ (отсюда $\varepsilon = 1/q$).

Доказательство. Пусть $A = GF(q) \times GF(q)$, $B = GF(q)$ и $H = \{h_{xyz} : x,y,z \in GF(q)\}$, где $h_{xyz}(a,b) = x + ay + bx$.

Теорема 6 [2, 9]. Пусть q будет степенью простого числа. Тогда существует $\varepsilon - SU(H,a,b)$ класс H хеш-функций от A до B, где $|A| = q^2$, $|B| = q$ и $|H| = q^2$ (отсюда $\varepsilon = 1/q$).

Доказательство. Пусть $A = B = GF(q)$ и $H = \{h_{xy} : x,y \in GF(q)\}$, где $h_{xy}(a) = x + ay$.

Рассмотрим некоторые методы комбинирования классов хеш-функций, которые обобщают сходные конструкции из [2 – 12].

Теорема 7 (Декартовое произведение) [2, 9]. Если существует $\varepsilon - U(H,a,b)$ класс H хеш-функций от A до B, тогда, для любого целого $i \geq 1$ существует $\varepsilon - U(H,a,b)$ класс H^i хеш-функций от A^i до B^i с $|H| = |H^i|$.

Доказательство: Для каждого $h \in H$ определим хеш-функцию $h^i : A^i \to B^i$ по правилу $h^i : (a_1,\ldots,a_i) = (h(a_1),\ldots,h(a_i))$. Определим $H^i = \{h^i : h \in H\}$.

Теорема 8 (Композиция 1) [2, 9]. Для i = 1, 2 предположим что существует $\varepsilon - U(H,a,b)$ класс H_i хеш-функций от A_i до B_i, где $A_2 = B_1$. Тогда существует $\varepsilon - U(H,a,b)$ класс H хеш-функций от A_1 до B_2, где $\varepsilon = \varepsilon_1 + \varepsilon_2$ и $|H| = |H_1| \times |H_2|$.

Доказательство. Для каждых $h_i \in H_i$, $i = 1,2$ определим хеш-функцию $h : A_1 \to B_2$ по правилу $h(a) = h_2(h_1(a))$. Пусть H будет множеством всех таких хеш-функций. Для двух любых входов вероятность коллизии не больше $\varepsilon_1 + (1 - \varepsilon_1)\varepsilon_2 < \varepsilon_1 + \varepsilon_2$

Теорема 9 (Композиция 2) [2, 9]. Предположим H_1 является $\varepsilon - U(H,a,b)$ классом хеш-функций от A_1 до B_1, и предположим H_2 является $\varepsilon - SU(H,a,b)$ классом хеш-функций от B_1 до B_2. Тогда существует $\varepsilon - SU(H,a,b)$ класс H хеш-функций от A_1 до B_2, где $\varepsilon = \varepsilon_1 + \varepsilon_2$ и $|H| = |H_1| \times |H_2|$.

Доказательство. Для каждых $h_i \in H_i$, $i = 1,2$ определим хеш-функцию $h : A_1 \to B_2$ по правилу $h(a) = h_2(h_1(a))$. Пусть H будет множеством всех таких хеш-функций. Пусть $x_1, x_2 \in A_1$ $(x_1 \neq x_2)$ и пусть $y_1, y_2 \in B_2$. Сколько функций в H отображают x_1 в y_1 и x_2 в y_2? Предположим, что $y_1 = y_2$. Тогда максимальное число коллизии не более

$$P|H_1| \times \frac{|H_2|}{b} + (1 - P)|H_1| \times \frac{\varepsilon_2 |H_2|}{b} \leq (\varepsilon_1 + \varepsilon_2)|H_1| \times \frac{|H_2|}{b}$$

Если $y_1 \neq y_2$, тогда число коллизий меньше. Поскольку $P \leq \varepsilon_1$, следует, что $\varepsilon - SU(H,a,b)$ класс с $\varepsilon_1 = \varepsilon_1 + \varepsilon_2$.

4. Применение универсального хеширования к аутентификации

Рассмотрим полученные конструкции для получения аутентификационных кодов.

Теорема 10 [2, 9]. Пусть q будет степень простого числа и пусть $i \geq 1$ будет целым числом. Тогда существует $\frac{i}{q} - U(H,a,b)$ q^i хеш-функций от A до B, где $|A| = q^{2^i}$ и $|B| = q$.

Доказательство. Применим доказательства теорем 4, 7 и 8.

Теорема 11 [2, 9]. Пусть q будет степень простого числа и пусть i ≥ 1 будет целым числом. Тогда существует $\frac{i+1}{q}-SU(H,a,b)$ класс q^{i+2} хеш-функций от A до B, где $|A|=q^{2^i}$ и $|B|=q$.

Доказательство: Применим доказательства теорем 6 и 9, 11.

Теорема 12 [2, 9]. Пусть q будет степень простого числа и пусть i ≥ 1 будет целым числом. Тогда существует $\frac{i}{q}+\frac{1}{q}-SU(H,a,b)$ класс q^{2i+3} хеш-функций от A до B, где $|A|=q^{2^i}$ и $|B|=q$.

Доказательство. Применим доказательства теорем 11 (с заменой q на q^2), 6 и 9.

Таким образом, представленные конструкции позволяют строить конструкции семейств универсальных и строго универсальных классов.

Рассмотрим практическое применение данных конструкций, используемых в самых быстрых алгоритм формирования MAC-кодов – UMAC-16 и UMAC-32.

5. Схемы формирования MAC-кодов, основанных на семействах универсальных хеш-функций

UMAC - код аутентификации сообщения был разработан Тедом Кроветцом (Ted Krovetz), Джоном Блэком (John Black), Шаи Халеви (Shai Halevi), Хьюго Кравцеком (Hugo Krawczyk) и Филиппом Рогэвеем (Phillip Rogaway) [13, 14]. Алгоритм основан на семействах универсальных хеш-функций и обеспечивает доказуемую безопасность MAC-кода, безопасность обеспечивается стойкостью применяемого блочно-симметричного шифра (БСШ) AES в режиме CBC (сцепления блоков открытого текста во втором слое функции Uhash-16 или Uhash-32).

Таким образом, алгоритм позволяет обеспечить более высокую скорость (особенно для длинных сообщений) и подтверждаемую безопасность ценой большей сложности.

Для описания процедур формирования MAC-кода рассмотрим UMAC (1999 года). Сообщение M произвольной длины поступает на двухслойную функцию Uhash, в которой на первом слое с помощью универсального класса хеш-функций NH сообщение разбивается на блоки определенной длины (за исключением последнего блока, который может иметь меньшую длину). Каждый блок обрабатывается аддитивным ключевым материалом (один ключ используется для каждого блока), процедура сжатия осуществляется путем умножения пары блока сообщения на ключ. Все сжатые блоки затем конкатенуются и длина информационного блока возрастает до установленного значения.

На втором слое с помощью функции PRF (псевдопроизвольной функции), используя либо режим CBC с БСШ AES, либо используя алгоритм HMAC, получаем MAC-код фиксированной длины. Таким образом, семейство универсальных хеш-функций NH используется как ускоритель на HMAC или CBC-MAC.

Кроме того, можно использовать конструкцию Тойплица (Toeplitz), для снижения вероятности подлога (применяя NH несколько раз с ключами, которые перемешаны между собой, и конкатенируя результаты), и/или использовать двухуровневое хэширование для уменьшения количества необходимых ключей. Существуют также некоторые другие вариации, позволяющие оптимизировать некоторые виды структур.

Значительная часть ограничений UMAC (1999 года) исходит из того, что сообщение сжатие до установленного коэффициента, а не установленной длины. В первом случае, код аутентификации вычисляется путем вычисления функции PRF(хеш||остаток), во втором случае может быть вычислен путем хеш⊕PRF(остаток), имеющий некоторые преимущества (использование PRF ограничено минимумом, у него нет входа неограниченной длины). NH, семейство универсальных хеш-функций, использованных в UMAC (1999 года), могло также

быть сжато до установленной выходной длины, в этом случае нужен будет ключ (сгенерированный PRG) длиной, равной сообщению (целое сообщение должно рассматриваться как единый блок в данном описании).

Новая версия UMAC (2000 года) является победителем криптографического европейского конкурса NESSI, вводит дополнительную сложность для решения проблемы сжатия сообщения до установленной длины так, что MAC может вычисляться хеш⊕PRF(остаток). Часть PRF работает кодируя остаток блочным шифром. Часть хэша (также называемая UHash) сжимает сообщение, состоящее из трех разных слоев:

- на первом слое используется быстрое семейство хеш-функций NH, для сжатия сообщения до установленного коэффициента.
- на втором слое хеш-код установленной длины использует семейство хеш-функций RP, которое не так быстро как NH, но генерирует выход установленной длины с использованием ключа установленной длины (для этого используется режим CBC БСШ AES).
- на третьем слое используется семейство хеш-функций IP, которое сводит длину своего входа до более подходящего размера.

Универсальное семейство хеш-функций RP основывается на полиномиальных вычислениях. Строка, состоящая из n слов длиной m бит может рассматриваться в качестве полинома степени n в области значений, где каждое слово строки служит коэффициентом. Для вычисления хэша необходимо вычислить полином для произвольно выбранной точки (ключа).

Для эффективности вычисления выполняются в области максимальных значений, однако меньше, чем 2^m. Функция применяется для расширения области до произвольной строки, при этом используется гибридная схема, в которой RP представляют собой полиномиальный хеш-код: небольшой диапазон значений используется для коротких сообщений, и больший – для более длинных сообщений. С точки зрения безопасности, вероятность коллизии несколько повышается по сравнению со слоем универсального класса хеш-функций NH алгоритма.

Слой с универсальным семейством хеш-функций IP сокращает длину своего входа поскольку слой хэша RP генерирует выходы, значительно большие по сравнению с предполагаемой вероятностью коллизий (для самых длинных аутентифицируемых сообщений большинство битов выходной строки слоя RP будут нулями).

6. Конструкции алгоритмов UMAC16 и UMAC32

Алгоритмы UMAC16 и UMAC32 основаны на трехслойных схемах хэша UHash16 и UHash32 соответственно и используют для кодирования остатка БСШ AES (Rijndael). При этом функция PRG, вычисляемая из ключа пользователя получает ключевое значение, необходимое во внутренней операции UHash и также основана на AES, в режиме обратной связи.

UHash16 использует 16-битовые слова, представляя их как подписанные целые. Слой хэша NH действует на блоках 2 Кб, сжатых в 32-битовые величины (соответствует коэффициенту сжатия 512). Вероятность ошибки оказалась не более 2^{15}. Результат проходит слой хэша RP, который вычисляет выходную строку установленной длины 128 бит. Семейство хеш RP является конструкцией, использовавшей три области значений с 32-битовыми, 64-битовыми и 128-битовыми первичными модулями соответственно. Длина сообщения ограничивается максимумом 2^{64} бит, и доказано, что этот слой незначительно увеличивает вероятность столкновения (около 2^{19}). Если аутентифицируемое сообщение достаточно небольшое, во-первых, отпадает необходимость в слое RP и данный слой пропускается в качестве оптимизации. Слой хэша IP добавляет свой 128-битовый ввод к 16-битовому выходу, создавая вероятность столкновения почти 2^{15}. Трехслойная конструкция повторяется множество раз, с независимыми ключами для увеличения длины кода

аутентификации и снижения шансов подлога MAC-кода. По умолчанию число повторений – четыре раза, и сложение 16-битовых выходных величин дает 64-битовый MAC-код с вероятностью подделки 2^{60}.

Основные различия с алгоритмом UHash32 заключаются в использовании 32-битовых слов и двукратном повторении трехслойной схемы (по умолчанию). Это дает различные возможности на практике (использование большей области значений), но анализ, главным образом, остается прежним.

Преимущества перед предыдущей версией UMAC (1999 года) заключается в использовании шифровального примитива (AES) минимизировано, что (в результате) дает большую эффективность для коротких сообщений и обеспечивает дополнительную гибкость верификации: можно выбрать количество параллельных итераций в вычислении MAC, тем самым варьируя вычислительным временем для обеспечения заданного уровня безопасности.

7. Сравнительный анализ хеш-функций

Одной из важнейших свойств хеш-функций является их защищенность от лобовой атаки. Это зависит от длины дайджеста (длины профиля). В таблице 1 представлены некоторые характеристики хеш-функций [1, 14].

Таблица 1

Хеш-функция	Класс функции	Базовые преобразования	Длина хеш, бит
Whirlpool	однонаправленная	в конечных полях Галуа	512
SHA-2	однонаправленная	логические и арифметические	256, 384, 512
ГОСТ 34311-95	однонаправленная	БСШ	256
HAVAL	однонаправленная	логические и арифметические	128, 160, 192, 256
SHA-1	однонаправленная	логические и арифметические	160
RIPEMD-160	однонаправленная	логические и арифметические	160
MD5	однонаправленная	логические и арифметические	128
MD4	однонаправленная	логические и арифметические	128
UMAC	однонаправленная (MAC)	в конечных полях Галуа	128, 64
Rijndael	выработка MAC	БСШ	128
ГОСТ 28147-89	выработка MAC	БСШ	64

Проведенный анализ табл. 1. показал, что хеш-функции с длиной профиля более 256 имеют большой запас стойкости, однако по скорости они уступают хеш-функциям с меньшей длиной профиля. В Украине в качестве государственного стандарта принят алгоритм ГОСТ 34311-95, однако данный алгоритм является одним из наиболее медленных алгоритмов. Напротив алгоритм UMAC обладает невысокой стойкостью, но зато имеет наивысшее быстродействие.

Для оценки сложности реализации хеш-функций была измерена скорость работы официальных реализаций на языке C, а также для сравнения некоторые оптимизированные версии с использованием языка assembler. В качестве компилятора использовался Microsoft Visual C++ 6.0. Тестирование скорости работы проводилось на компьютерах Pentium III 1000 MHz, 256 MB RAM под управлением операционной системы Microsoft Windows 2000 Professional. Результаты тестирования скорости работы алгоритмов хэширования представлены в табл. 2.

Анализ табл. 2 показал, что алгоритм UMAC поддерживает два режима работы: однонаправленная хеш-функция и функция выработки MAC-кодов, обладает невысокой стойкостью, но зато имеет наивысшее быстродействие, приближающееся к 6 Гбит/с на процессоре Pentium III 1000 MHz.

Таблица 2

Функция хеширования	Количество циклов	Язык реализации	Скорость работы на Pentium III 1000 MHz (Мбит/с)
Whirlpool	10	C	46,961
SHA-2 (512)	80	C	68,701
SHA-2 (256)	64	C	135,557
ГОСТ 34311	-	C+Assembler	83,056
HAVAL	96 (160)	C	564,809
SHA-1	80	C Assembler	344,433 605,558
RIPEMD-160	160	C	246,568
MD5	64	C	574,635
MD4	48	C	467,793
UMAC	-	C C+Assembler	1648,953 5885,057
Rijndael CBC–MAC	14	C	231,255
ГОСТ 28147 (режим 4)	16	C+Assembler	315,270

Выводы

Таким образом, код аутентификации сообщения UMAC, основанный на семействах универсальных хеш-функций, обеспечивает доказуемую безопасность, основанную на стойкости шифровального примитива, использованного для кодирования остатка (AES (Rijndael)). Однако применяемые методы универсального хеширования не позволяют обеспечить криптографическую стойкость к атакам злоумышленника. Практически все функции универсального хеширования применяются в композиции с алгоритмами шифрования, в результате чего обеспечивается стойкость, но теряется свойство универсальности.

Перспективным направлением дальнейших исследований разработка новых подходов к формированию стойких универсальных схем хеширования, исследование эффективных методов и алгоритмов их применения для обеспечения целостности и аутентичности информации.

Список литературы

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е И. – М.: Вильямс, 2001. – 672 с

2. J. L Carter and M. N. Wegman. Universal classes of hash functions, J. Corn-put. System Sci. 18 (1979), C. 143-154.

3. R. L. Plackett and J. P. Burman. The design of optimum multi-factorial experiments, Biometrika33 (1945), C. 305-325.

4. D. V. Sarwate. A note on universal classes of hash functions, Inform. Proc. Letters 10 (1980), 41-45.

5. G. J. Simmons. Message authentication: a game on hypergraphs, Congr. Numer. 45 (1984), 161-192.

6. G. J. Simmons. A survey of information authentication, Proc. of the IEEE 76 (1988), 603-620.

7. D. R. Stinson. Some constructions and bounds for authentication codes, J. Cryptology 1 (1988), 37-51.

8. D. R. Stinson. The combinatorics of authentication and secrecy codes, J. Cryptology 2 (1990), 23-49.

9. D. R. Stinson. Combinatorial techniques for universal hashing, submitted to J. Comput. System Sci.

10. D. R. Stinson. Combinatorial characterizations of authentication codes, submitted to Designs, Codes and Cryptography (a preliminary version appears elsewhere in these proceedings).

11. M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality, J. Comput. System Sci. 22 (1981), 265-279.

12. Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993.

13. Cryptrec. Cryptrec liaison report to ISO/IEC 18033-2 and 18033-3. Technical report, ryptography Research and Evaluation Committees, October 2002.

14. Jakob Jonsson and Burt Kaliski. RSA-PSS. Primitive submitted to NESSIE by RSA,September 2000.

Поступила 23.01.09

УДК 681.3.004

Петров А.А.

ОПРЕДЕЛЕНИЯ ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК СИСТЕМ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Под техническими характеристиками (ТХ) систем активной защиты будем понимать ряд важнейших качеств данной системы, определяющих эффективность ее применения как средства защиты информации от утечки за счет ПЭМИН. К числу таких характеристик могут быть отнесены:

1) маскировочная способность;
2) защищенность по отношению к методам селекции и компенсации помех;
3) скрытность применения;
4) универсальность;
5) соответствие требованиям электромагнитной совместимости;
6) простота технической реализации.

Маскирующая способность систем активно защиты (САЗ) характеризует степень подавления приемника перехвата искусственной помехой и зависит, в первую очередь, от применяемого класса помех, что определяет потенциальные возможности САЗ, а также от полноты технической реализации предложенной математической модели помехи. Эта характеристика требует качественного описания и должная позволять сравнивать достигнутую за счет применения САЗ защищенность канала утечки с установленными нормами на границе контролируемой зоны.

Естественным количественным показателем, наиболее полно отражающим маскирующую способность помехи, является средняя вероятность ошибки при приеме одного бита информации. Именно эта величина нормируется в качестве первичной в действующей и последующих редакциях норм, поскольку она определяет возможность восстановления перехваченной информации. Вероятность ошибки во многом зависит от способа приема, и для создания гарантированного уровня защищенности принято исходить из предположения, что техническая разведка пользуется оптимальными методами приема и, тем самым, может минимизировать величину средней вероятности ошибки.

Изложенной соображение предполагает метод количественной оценки маскирующей способности помех, заключающейся в следующем:

1. С учетом действующих в канале утечки сигналов и помех формируется математическая