Так как вычисление числа классов в общем случае трудоемкий процесс, то определение d_{def}, т. е. числа классов мнимого квадратичного поля $Q\left(\sqrt{\Delta}\right)$, где $\Delta=(q+1-\#E(F_q))^2-4q$, требует экспоненциальное время. Поэтому можно только проверить, что число классов достаточно большое.

Существует эффективное постоянное c_1 такое, что для функционального дискриминанта Δ_f число классов поля $Q\left(\sqrt{\Delta_f}\right)$ удовлетворяет неравенству

$$h\left(\Delta_f\right) \geq \frac{c_1\sqrt{\left|\Delta_f\right|}}{log\,log\left|\Delta_f\right|}$$

Следовательно, для проверки условия (6) необходимо вычисление свободной от квадратов части Δ. В настоящее время наилучший алгоритм для решения этой проблемы включает факторизацию числа Δ. После этого можно проверить условие (6) используя вышеприведенную нижнюю границу для $h(\Delta_f)$.

Вычисления числа классов тестовых ЭК, приведенных в стандарте [3], показали, что хотя в этом стандарте не требуется проверка условия (6), тем не менее это условие удовлетворяется.

1. Ростовцев А.Г., Маховенко Е.Б., Введение в криптографию с открытым ключом – С.-П.: Мир и семья, 2001. – 336 с.
2. Baier H., Buchmann J., Efficient construction of crypto-graphically strong elliptic curves, Progress in Cryptology –INDOCRYPT'2000, LNCS Vol.1977, Springer-Verlag, 2000, p.191-202.
3. National Institute of Standards and Technology, NIST: FIPS Publication 186-2: Digital Signature Standard (DSS), January 2000.

ОБ ОДНОЙ МОДЕЛИ РАЗМЕЩЕНИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ ВО ВЗАИМОУВЯЗАННЫХ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ ПРОСТРАНСТВАХ

Шыхалиев Р.Г.

Институт Информационных Технологий НАН Азербайджана, Баку,

E-mail: secretary@iit.ab.az

Сегодня корпоративные информационно-телекоммуникационные системы функционируют в основном в интересах определенных корпораций, предприятий и организаций и, как правило, разобщенно. При этом корпоративная разобщенность затрудняет обмен информацией и доступ к ней. Для интегрирования корпоративных информационных пространств необходимо обеспечение взаимоувязанности этих информационных пространств. Взаимоувязанность корпоративных информационных пространств необходима для обеспечения структурной и функциональной целостности единого корпоративного информационного пространства, полученного в результате интеграции различных корпоративных информационных пространств. При этом обеспечение информационной безопасности является одной из главных задач, которую необходимо решать.

Одним из средств обеспечения информационной безопасности является межсетевой экран (МЭ).

В этой работе наше исследование сосредотачивается на задаче размещения МЭ во взаимоувязанных корпоративных информационных пространствах.

Постановка задачи. Пусть, имеется n МЭ $FW_1, FW_2, ..., FW_n$ и m узлов с критической информацией $U_1, U_2, ..., U_m$. Известна мера r_{ij} ущерба при использовании FW_i для защиты U_j $(i=\overline{1,n}; j=\overline{1,m})$. Требуется организовать такое размещение МЭ, при котором суммарный ущерб будет минимальным.

Построим математическую модель этой задачи. Для этого отношение между элементами FW и U зададим булевой матрицей x_{ij} которая описывается следующим образом:

Пусть $$X_{ij} = \begin{cases} 1, \text{ если } F_i \text{ используется для защиты } U_j \\ 0, \text{ если } F_i \text{ не используется для защиты } U_j. \end{cases}$$

Рассмотрим булеву матрицу (x_{ij}) размера $m \times n$, такую, что:

$$\sum_{i=1}^{n} x_{ij} \le 1 \ \left(j=\overline{1,m}\right), \quad \sum_{j=1}^{m} x_{ij} \le 1 \ \left(i=\overline{1,n}\right),$$
$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} \le \min(n,m) \tag{1}$$

При этих условиях (x_{ij}) можно называть матрицей размещения МЭ. Среди (x_{ij}) надо выбрать такие, для которых в (1) достигается равенство. При этом эти (x_{ij}) называются насыщенными.

Стоимость любой матрицы размещения (x_{ij}) выражается суммой $F = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij} x_{ij}$.

Окончательно математическая модель задачи размещенчя МЭ будет такой.

Найти матрицу $X = \left(x_{ij}\right)$ $\left(i=\overline{1,n} \ ; \ j=\overline{1,m}\right)$ такую, что :

$$F(X) = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij} x_{ij} \to \min \tag{2}$$

при условиях

$$\sum_{i=1}^{n} x_{ij} \le 1 \ \left(j=\overline{1,m}\right); \quad \sum_{j=1}^{m} x_{ij} \le 1 \ \left(i=\overline{1,n}\right) \tag{3}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} = \min(n,m) \tag{4}$$

$$x_{ij} \in \{0,1\} \ \left(i=\overline{1,n}; \ j=\overline{1,m}\right) \tag{8}$$

Другими словами, ищется насыщенная матрица размещений МЭ, оптимизирующая форму F.

1. Алгулиев Р.М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей. - М.: УРСС, 2001. -247с.
2. Зайченко Ю.П. Исследование операций: Учеб. пособие для студентов вузов. - Киев: Вища школа. 1979. -392с.

ИССЛЕДОВАНИЕ ОЦЕНОЧНЫХ ТЕСТОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ахадова З.М.

Институт Информационных Технологий НАН Азербайджан, Баку
E-mail: zehraLMN@mail.ru

Случайные числа и их генераторы являются неотъемлемыми элементами современных криптосистем. Проблема генерации случайной последовательности с произвольным законом распределения вероятностей сводится к проблеме генерации равномерно распределенной случайной последовательности (РРСП). РРСП, это, случайная последовательность $x_1, x_2, \ldots, x_t, x_{t+1}, \ldots$ со значениями в дискретном множестве $A=\{0,1,\ldots, N\text{-}1\}$, определенная на вероятностном пространстве (Ω, F, P) и удовлетворяющая двум следующим свойствам [1]:

1. Для любого $n \in \mathrm{N}$ и произвольных значений индексов $1 \leq t_1 < \ldots < t_n$ случайные величины $x_{t_1}, \ldots, x_{t_n} \in A$ независимы в совокупности.
2. Для любого номера $t \in \mathrm{N}$ случайная величина x_t имеет дискретное равномерное на A распределение вероятностей: $\mathrm{P}\{x_t = i\} = 1/N,\ i \in A$.

Так как чрезвычайно сложно формировать случайных последовательностей, на практике используют качественные псевдослучайные последовательности (ПСП), которые по своей сути являются детерминированными, в то же время обладают статистическими свойствами близкими к свойствам случайных последовательностей.

Стойкость криптосистем существенно зависит от того, насколько точно соответствует используемая последовательность $x_t \in A$ $(t=1, 2, \ldots)$ модели РРСП. Проверка близости $\{x_t\}$ к модели РРСП осуществляется методами статистического тестирования и состоит в проверке гипотез выполнения выше указанных базовых свойств РРСП.

С целью выявления наиболее качественных наборов тестов было проведено исследование оценочных тестов, используемых для анализа статистической безопасности генераторов ПСП, ориентированных на использование в системах криптографической защиты. Были проанализированы следующие тесты:

– Универсальный алгоритм тестирования [2].

– Классические тесты: проверка несцепленных серий, проверка интервалов, проверка комбинаций, тест собирателя купонов, тест *n*-серий, обобщенный покер-тест, проверка перестановок, проверка на монотонность, проверка корреляции [3]