Секция «Дискретная математика и математическая кибернетика»

# Критерий отсутствия скрытых каналов передачи информации

***Гукасян Вагаршак Грачикович***

*Аспирант*

Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра математической теории
интеллектуальных систем, Москва, Россия

*E-mail: vagarsh.guv@mail.ru*

В данной работе расширены результаты работы [1] по анализу информационных систем на наличие скрытых каналов передачи информации. В работе [1] вводится следующая модель двухуровневой компьютерной системы:

Система моделируется абстрактным автоматом $A = (X, S, Y, \delta, \lambda)$, где $X, S, Y$ — конечные непустые множества, соответственно, входной алфавит, множество состояний и выходной алфавит, $\delta : X \times S \to S$ — функция переходов, $\lambda : X \times S \to Y$ — функция выходов.

Пусть $X = X_H \times X_L$, где $X_H$ и $X_L$ — множества входов для пользователей уровней $H$ (High) и $L$ (Low). Аналогично, $S = S_H \times S_L$, $Y = Y_H \times Y_L$.

**Определение 1.** Пусть $s^1, s^2 \in S$. Положим $s^1 \sim s^2$, если $s^1_L = s^2_L$. Обозначим $S/_\sim$ фактор-множество относительно отношения $\sim$; $[s]$ — класс эквивалентности, содержащий $s$, $s \in S$.

Аналогично определим отношение эквивалентности на $Y$.

**Определение 2.** Будем говорить, что $L$ не видит $H$, если
функция $\tilde{\delta} : X_L \times S/_\sim \to S/_\sim$, определяемая формулой

$$\tilde{\delta}(X_L, [s]) = [\delta((x_H, x_L), s')],\ x_H \in X,\ s' \in [S],$$

и функция $\tilde{\lambda} : X_L \times S/_\sim \to Y/_\sim$, определяемая формулой

$$\tilde{\lambda}(X_L, [s]) = [\lambda((x_H, x_L), s')],\ x_H \in X,\ s' \in [S],$$

корректно определены.

Пусть на множестве $X = X_H \times X_L$ задано вероятностное распределение $P$. При каждом фиксированном состоянии $s$ распределение $P$ индуцирует на $Y$ распределение вероятностей $Q^s$:

$$Q^s(y) = P\{x \in X : \lambda(x, s) = y\}.$$

Тогда совместная вероятность на $X_H \times Y_L$ имеет вид:

$$P^s(x^0_H, y^0_L) = P\{(x^0_H, x_L) : x_L \in X_L, \lambda((x^0_H, x_L), s) = (y_H, y_L), y_H \in Y_H\}.$$

А условная вероятность записывается как $P^s(y_L|x_H) = \frac{P^s(x_H, y_L)}{P_H(x_H)}$

**Определение 3.** Пусть $L$ не видит $H$. Скажем, что $L$ не видит $H$ по вероятности, если для всех $x_H \in X_H$, $y_L \in Y_L$, $[s] \in S/_\sim$

$$P^{s^1}(y_L|x_H) = Q^{s^2}(y_L),\ s^1, s^2 \in [s]$$

Основной результат работы [1]:

**Теорема 1.** *Пусть $L$ не видит $H$. Тогда для невидимости по вероятности достаточно, чтобы для всех $x \in X$ выполнялось равенство*

$$P(x_H, x_L) = P_H(x_H)P(x_L).$$

Основным результатом данной работы является критерий существования невидимости по вероятности. Чтобы его сформулировать, дополнительно вводятся определения ниже.

Для каждого $s$ функция $\lambda(x, s)$ разбивает $X_L$ на классы эквивалентности:

**Определение 4.** Пусть $L$ не видит $H$ и зафиксировано состояние $s \in S$. Будем называть $L$-входы $x_L^1, x_L^2 \in X_L$ эквивалентными, если соответствующие им $L$-выходы равны:

$$x_L^1 \overset{s}{\sim} x_L^2 \Leftrightarrow \forall x'_H, x''_H \in X_H : \lambda((x'_H, x_L^1), s) = \lambda((x''_H, x_L^2), s).$$

Обозначим $X_L/_{\overset{s}{\sim}}$ за $\overline{X}_L^s$. Отметим, что распределение вероятностей на $X_L$ индуцирует распределение вероятности на $\overline{X}_L^s$.

**Теорема 2.** *Пусть $L$ не видит $H$. Вероятностное невлияние имеет место тогда и только тогда, когда для любого состояния $s$ вероятностные распределения на $X_H$ и $\overline{X}_L^s$ независимы.*

Также в данной работе доказано следующее утверждение:

**Следствие 1.** *Независимость распределений на $X_H$ и $X_L$ не является необходимым условием вероятностного невлияния.*

### Источники и литература

1) Грушо А. А., Шумицкая Е. Л. Модель невлияния и скрытые каналы, Дискретная математика, 2002, Т. 14, № 1, С. 11–16