которых должно быть однозначно сопоставимо с реальными объектами, действиями и процессами. Выполнение данного требования позволяет избежать возможности неоднозначной трактовки правил политики ИБ;

— *Поддержка широкого спектра правил политики ИБ*. Чем шире этот спектр, тем более универсальным является язык;

— *Применимость к конкретным системам*. Правила политики ИБ, формализованные с помощью языка, должны быть транслируемы в форматы данных и языки конкретных систем. Выполнение этого требования позволяет решить проблему реализации политики ИБ в качестве конфигурации различных систем безопасности;

— *Расширяемость*. Язык должен быть формализован таким образом, чтобы при добавлении нового типа правил ИБ в спецификацию языка общая структура предложений языка оставалась неизменной. Выполнение данного требования позволяет сделать язык применимым к большему числу типов политик и систем путем его расширения;

— *Открытость спецификации*. Выполнение данного требования обеспечивает возможность расширения языка и его применения к конкретным системам не только разработчиком языка, но и другими заинтересованными сторонами.

СПИСОК ЛИТЕРАТУРЫ:

1. *Thayer R.* Network Security: Locking in to Policy // Data Communications. 1988. № 4.
2. *Chernyavskiy D., Miloslavskaya N.* Unified Language for Network Security Policy Implementation // Proceedings of ICNS 2011: The Seventh International Conference on Networking and Services. 2011.
3. ГОСТ ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
4. *Dongliang J., Lianzhong L., Shilong M., Xiaoni W.* Research on Security Policy and Framework // Proceedings of the Second International Symposium on Networking and Network Security (ISNNS10). 2010.

В. Б. Щербаков

МЕТОДИКА РИСК-АНАЛИЗА ПРОЦЕССА ПЕРЕХВАТА РАДИОСИГНАЛОВ БЕСПРОВОДНОЙ СЕТИ

Существуют различные подходы к определению мер риска, существенно зависящие от методики оценки их значений. Исходя из этих мер могут быть получены некоторые прогнозные оценки.

Для риск-анализа процесса перехвата радиосигналов беспроводной сети предлагается методический подход, основанный на следующих показателях: гипотеза H_0 соответствует отсутствию сигнала на входе приемника; гипотеза H_1 — наличию сигнала; γ_0 — решение принять гипотезу H_0; γ_1 — решение принять гипотезу H_1. Ущерб предлагается оценивать величиной $\frac{Y_{ñø}}{N_0}$, где $Y_{ñø}$ — накопленная энергия смеси сигнала и шума, а N_0 — спектральная плотность мощности шума.

Тогда введем понятие матрицы ущербов:

$$C = \begin{pmatrix} C_{00} & C_{01} \\ C_{10} & C_{11} \end{pmatrix}, C_{01} > C_{00} \geq 0, C_{10} > C_{11} \geq 0, \quad (1)$$

где на главной диагонали расположены ущербы за правильные решения, на побочной — за ошибки первого и второго рода соответственно [1].

Кроме того, известны априорные вероятности гипотезы H_0 и альтернативы H_1, которые образуют полную группу событий:

$$p_0 = P(H_0) = 1 - P(H_1) = 1 - p_1. \quad (2)$$

Вероятность ошибки α первого рода определяется следующим образом:

$$\alpha = P(\gamma_1 \mid H_0) = P(x \in X_1 \mid H_0) = \int_{X_1} W(x \mid H_0)dx. \quad (3)$$

Вероятность правильного решения, состоящего в принятии верной гипотезы H_0, равна

$$P(\gamma_0 \mid H_0) = P(x \in X_0 \mid H_0) = \int_{X_0} W(x \mid H_0)dx = 1 - \int_{X_1} W(x \mid H_0)dx = 1 - \alpha. \quad (4)$$

Вероятность β ошибки второго рода

$$\beta = P(\gamma_0 \mid H_1) = P(x \in X_0 \mid H_1) = \int_{X_0} W(x \mid H_1)dx. \quad (5)$$

Вероятность правильного решения, состоящего в отклонении ложной гипотезы, находится [1]

$$P(\gamma_1 \mid H_1) = P(x \in X_1 \mid H_1) = \int_{X_1} W(x \mid H_1)dx = 1 - \int_{X_0} W(x \mid H_1)dx = 1 - \beta. \quad (6)$$

Вероятность α ошибки первого рода в математической статистике называют уровнем значимости, а вероятность $1 - \beta$ отвергнуть ложную гипотезу — мощностью правила выбора решений.

Априорные вероятности γ_0 и γ_1

$$P(\gamma_0) = p_0 P(\gamma_0 \mid H_0) + p_1 P(\gamma_0 \mid H_1) = p_0(1 - \alpha) + p_1 \beta; \quad (7)$$

$$P(\gamma_1) = p_0 P(\gamma_1 \mid H_0) + p_1 P(\gamma_1 \mid H_1) = p_0 \alpha + p_1(1 - \beta). \quad (8)$$

определяют частоты появления отдельных решений в длинной последовательности принятия решений. В (7), (8) $p_1\beta$, $p_0\alpha$ — априорные вероятности ошибок, а $p_0(1-\alpha)$, $p_1(1-\beta)$ — априорные вероятности правильных решений [2, 3].

Используя указанный комплект исходных данных, запишем выражения среднего риска для пользователя беспроводной сети и человека, осуществляющего перехват радиосигналов соответственно [2, 3]

$$R_0 = p_0 C_{00} P(\gamma_0 \mid H_0) + p_1 C_{11} P(\gamma_1 \mid H_1) = p_0 C_{00}(1-\alpha) + p_1 C_{11}(1-\beta); \quad (9)$$

$$R_1 = p_0 C_{01} P(\gamma_1 \mid H_0) + p_1 C_{10} P(\gamma_0 \mid H_1) = p_0 C_{01}\alpha + p_1 C_{10}\beta. \quad (10)$$

Рассмотрим на примере применение предлагаемой методики риск-анализа процесса перехвата радиосигналов беспроводных сетей стандарта IEEE 802.11a. В качестве исходных данных могут применяться результаты имитационного моделирования анализируемого процесса.

Пусть в некоторой реализации модели (рис. 1) значения порога принятия решения $K_0 = 0,009047$ при отношении сигнал/шум $\frac{P_c}{P_ш} = \frac{0,103}{4} = 0,02575$ вероятность ложной тревоги составляет $Q_F \approx 10^{-3}$, вероятность правильного обнаружения — $Q_D = 0,322$. Следовательно, вероятность правильного необнаружения составляет $Q_{пп} = 0,999$, вероятность неправильного обнаружения составляет $Q_{перов} = 0,678$.

Тогда априорные вероятности гипотез будут иметь следующие значения:

$$P(H_0) = 0,4;\ P(H_1) = 1 - 0,4 = 0,6.$$

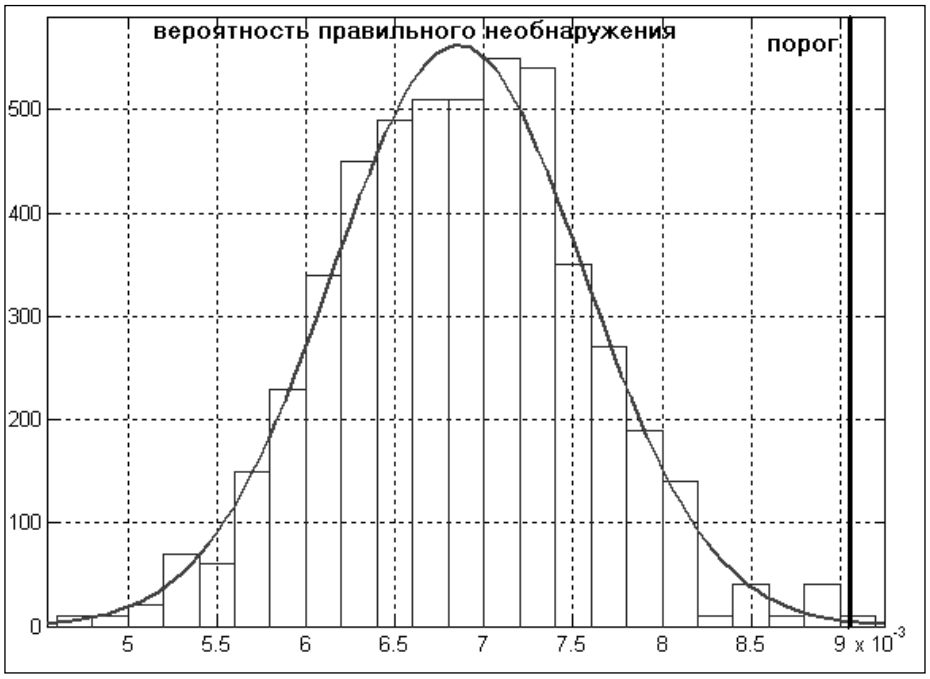

Рис. 1. Гистограмма значений отношения накопленной энергии шума за время $T = 0{,}02$ с к спектральной плотности мощности шума

Таблица 1. Расчет основных показателей риска

Показатель	Значение
C_{00}	$6{,}5 \cdot 10^{-3}$
C_{01}	$9{,}8 \cdot 10^{-3}$
C_{10}	$8{,}5 \cdot 10^{-3}$
C_{11}	10^{-2}
R_0	0,0045294
R_1	0,00346172

В таблице приведены результаты расчета основных показателей риска, полученные в соответствии с предлагаемой методикой для смоделированного процесса перехвата радиосигналов беспроводных сетей стандарта IEEE 802.11a.

Таким образом, разработанная методика открывает возможность проведения аналитического риск-анализа процесса обнаружения беспроводных сетей и перехвата циркулирующей в них информации, а также дополняет разрабатываемую методологию [4] построения риск-шанс-моделей беспроводных сетей группы стандартов IEEE 802.11.

СПИСОК ЛИТЕРАТУРЫ:

1. *Левин Б. Р.* Теоретические основы статистической радиотехники. 3-е изд., перераб. и доп. М.: Радио и связь, 1989. — 656 с.
2. *Вентцель Е. С.* Теория вероятностей: Учеб. для вузов. 7-е изд. М.: Высш. шк., 2001. — 575 с.
3. *Гмурман В. Е.* Теория вероятностей и математическая статистика: учеб. пособие. 12-е издание, перераб. М.: Высшее образование, 2008. — 479 с.
4. *Щербаков В. Б.* Безопасность беспроводных сетей: стандарт IEEE 802.11 / В. Б. Щербаков, С. А. Ермаков; под ред. В. И. Борисова. М.: РадиоСофт, 2010. — 256 с.