

Татьяна Юрьевна ЗЫРЯНОВА —
 специалист организационно-аналитического отдела
 управления информатизации
 Уральского государственного университета
 путей сообщения

УДК 004.056.53

МЕТОД ОПРЕДЕЛЕНИЯ УРОВНЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

АННОТАЦИЯ. В работе предложен математический метод определения уровней выполнения функций защиты информации и уровня обеспечения защиты информации в целом. В качестве основы для определения этих значений используется метод построения функций надежности.

In the presented article the mathematical method of definition of levels of functions of information security is offered. As a basis for definition of these values the method of construction of functions of reliability is used.

В качестве исходного множества функций защиты информации рассмотрим множество, приведенное в [1]:

Функция f_1 . Предупреждение условий, порождающих дестабилизирующие факторы (ДФ).

Функция f_2 . Предупреждение проявления ДФ.

Функция f_3 . Обнаружение проявившихся ДФ.

Функция f_4 . Предупреждение воздействия ДФ на информацию.

Функция f_5 . Обнаружение воздействия ДФ на информацию.

Функция f_6 . Локализация воздействия ДФ на информацию.

Функция f_7 . Ликвидация последствий воздействия ДФ на информацию.

Введем определение *уровня выполнения функции защиты информации*. Уровнем выполнения i -той функции защиты информации $Y_i(t)$, $i=1, \dots, 7$, будем называть вероятность того, что i -тая функция защиты информации будет выполняться в течение периода времени длительностью t .

Тогда, исходя из соотношения:

$$p(t) = \lambda(1 - P(t)), \quad (1)$$

где $p(t)$ — вероятность того, что условия, порождающие ДФ, возникнут в момент времени t , $P(t)$ — вероятность того, что условия, порождающие ДФ, не возникли до момента времени t , λ — коэффициент пропорциональности, можно доказать, что время, на протяжении которого функция 1 выполняется, имеет экспоненциальное распределение с функцией распределения:

$$F(t) = 1 - e^{-\lambda t}. \quad (2)$$

Следовательно, уровень выполнения функции 1 определяется по формуле:

$$Y_1(t) = e^{-\lambda t}, \quad (3)$$

то есть является функцией надежности для функции 1.

Как известно [2], математическое ожидание случайной величины, распределенной по экспоненциальному закону, равняется $1/\lambda$. Следовательно, в качестве коэффициента пропорциональности λ может быть использована статистическая оценка (выборочное среднее) среднего времени до возникновения условий, порождающих ДФ \bar{T}_1 . Окончательная формула для определения уровня выполнения функции 1:

$$Y_1(t) = e^{-\frac{t}{\bar{T}_1}} \quad (4)$$

Значение \bar{T}_1 — это значение, которое необходимо знать для вычисления $Y_1(t)$. Назовем его *исходным показателем защищенности для функции 1*. В дальнейшем будет построено множество таких показателей для системы защиты информации в целом.

Кроме того, зная $Y_1(t)$, можно вычислить вероятность того, что выполнение функции 1 прекращается в момент времени t , $P_1(t) = 1 - Y_1(t)$. Будем называть $P_1(t)$ *остаточной вероятностью для функции 1*. Эту вероятность также будем рассматривать в качестве элемента системы показателей защищенности, но подобные показатели отнесем к множеству *результатирующих показателей*.

Для остальных функций защиты информации определение уровней выполнения проводится аналогичным образом, но с учетом того, что предыдущая функция защиты не выполнена. В результате уровни выполнения $Y_i(t)$ для $i=2, \dots, 7$ вычисляются по формулам:

$$Y_i(t) = 1 - \prod_{j=1}^i \left(1 - e^{-\frac{t}{\bar{T}_j}} \right), \quad i=2, \dots, 7. \quad (5)$$

Здесь \bar{T}_i — статистические оценки средних временных интервалов выполнения функций защиты со второй по седьмую.

Кроме того, формула:

$$Y_7(t) = 1 - \prod_{j=1}^7 \left(1 - e^{-\frac{t}{\bar{T}_j}} \right) \quad (6)$$

определяет уровень обеспечения защиты информации в целом.

Аналогично функции 1 для остальных функций определяется и остаточная вероятность по формуле:

$$P_i(t) = 1 - Y_i(t) \quad i=2, \dots, 7. \quad (7)$$

Следует отметить, что в случае, когда воздействие ДФ на информацию не локализовано и не ликвидировано, возникает ущерб от нарушения информационной безопасности. Оценки ущерба обозначим M_6 для функции 6 и M_7 для функции 7. Оценки ущерба, так же как и оценки временных интервалов, относятся к множеству исходных показателей защищенности информации.

Зная остаточную вероятность для функции 6 и 7 $P_6(t)$ и $P_7(t)$, а также оценки ущерба M_6 и M_7 , можно определить информационный риск, возникающий вследствие невыполнения функций 6 и 7 следующим образом:

$$R_6(t) = P_6(t) \cdot M_6; \quad (8)$$

$$R_7(t) = P_7(t) \cdot M_7. \quad (9)$$

Итак, нами построены:

1. множество исходных показателей защищенности информации $\{\bar{T}_1, \bar{T}_2, \bar{T}_3, \bar{T}_4, \bar{T}_5, \bar{T}_6, \bar{T}_7, M_6, M_7\}$;
2. формулы для определения уровней выполнения функций защиты информации $\{Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7\}$;
3. множество производных показателей защищенности информации $\{P_1, P_2, P_3, P_4, P_5, P_6, P_7, R_6, R_7\}$.

Применение предложенного метода предполагает:

- 1) получение оценок исходных показателей защищенности информации;
 - 2) вычисление уровней выполнения функций защиты и остаточных вероятностей;
 - 3) вычисление значений производных показателей защищенности информации.
- Значения Y_7, P_7, R_7 определяют соответственно уровень обеспечения защиты, вероятность необеспечения защиты и информационный риск для системы защиты информации в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Герасименко В. А., Малюк А. А. Основы защиты информации. М., 1997. 537 с.
2. Гмурман В. Е. Теория вероятностей и математическая статистика. М., 2002. 479 с.

Александр Анатольевич ЗАХАРОВ —
зав. кафедрой информационной безопасности,
доктор технических наук, профессор

Евгений Александрович ОЛЕННИКОВ —
доцент кафедры информационной безопасности,
кандидат технических наук

Алексей Сергеевич ПЕТУХОВ —
аспирант кафедры информационной безопасности

УДК 004.94:61

ИНФОРМАЦИОННАЯ МОДЕЛЬ ЭЛЕКТРОННОЙ ИСТОРИИ БОЛЕЗНИ ПАЦИЕНТА

АННОТАЦИЯ. В статье описывается информационная модель хронологических деревьев, применяемая для внутреннего представления электронной истории болезни пациента с целью решения задачи отбора актуальной информации.

The article describes the informational model of chronological trees. This model is used for the internal presenting of electronic history of patient disease with the purpose of important information selection.

Объем хранимой медицинской информации в современном медицинском учреждении, необходимость снижения затрат на оперативную обработку данных и совершенствование форм их представления явились предпосылками создания медицинских информационных систем (МИС), в основу которых положены алгоритмы структурной организации данных в виде электронных историй болезни пациентов.