УДК 004.056.53

МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЧЕТКИХ МНОЖЕСТВ

Бусько Михаил Михайлович, к.т.н., доцент
Байкальский государственный университет, г. Иркутск
Busko Mikhail, PhD, buskomm@bgu.ru
Baikal State University

Рассматривается возможность формализации процесса моделирования нарушителя информационной безопасности с применением теории нечетких множеств. Такое представление экспертных оценок позволит автоматизировать трудоемкий процесс моделирования и снизить субъективность.

Ключевые слова: *информационная безопасность, информационная система, модель нарушителя, нечеткие множества, нечеткая логика.*

При проектировании системы защиты информации необходимо построение модели угроз и оценка риска информационной безопасности. Идентификация каждой угрозы предполагает обязательное определение источника угроз. Источники угроз классифицируются, как антропогенные, техногенные и стихийные. Для рассмотрения антропогенных источников строится модель потенциального нарушителя.

Множество существующих подходов основываются на либо неформальном описании характеристик нарушителя в качественных оценках, либо на количественных значениях, характеризующих взаимодействие нарушителя с защищаемым объектом. В первом случае применяются вербальные градации (технических знаний, оснащенности, возможностей по доступу и др.) субъективных экспертных оценок [1,2]. Любая же экспертная оценка обладает большой трудоемкостью и связана с необходимостью привлечения в качестве экспертов квалифицированных специалистов. Во втором случае получают формализованное описание сценариев реализации несанкционированных действий, дающих чаще всего вероятностные количественные значения [2]. Такой подход к моделированию не позволяет учесть достаточно много факторов, многие из которых не поддаются формализованному описанию. Следует так же отметить, что не все угрозы носят вероятностный характер в силу высокой их неопределенности, это в первую очередь относится к цели или мотивации нарушителя для совершения каких–либо действий [3,4].

В настоящей работе предлагается к рассмотрению возможность применения теории нечетких множеств для формального описания нарушителя информационной безопасности. В качестве обобщенного показателя, который наиболее подходит для характеристики возможностей нарушителей к выполнению несанкционированных действий примем «потенциал нападения» согласно

[5]. Данный показатель определяется на основании экспертных оценок частных факторов в качественных значениях, которые затем сопоставляются количественным, суммируются, а сумма опять переводится в качественную характеристику. Имея такую сложную цепочку преобразований можно утверждать, что оценка «потенциала нападения» может быть сделана только с большой неопределенностью.

Заключение о «потенциале нападения» эксперт делает на основании анализа пяти факторов [5]. Для каждого фактора определена качественная шкала и их можно рассматривать как множества носители лингвистических переменных. Каждой лингвистической переменной сопоставляется числовая переменная, принимающая свои значения на определенном числовом промежутке. В нашем случае значения лингвистических переменных уместно рассматривать, как нечеткие числа с треугольной функцией принадлежности. Полученные числовые промежутки расширяют возможности эксперта и позволяют ему более гибко проводить оценку, задействовав промежуточные значения. Треугольная функция принадлежности в общем случае может быть задана аналитическим выражением или определена тремя числами $\mu_{\Delta} = (a_1; a_2; a_3)$. Введем для каждого фактора лингвистические переменные, зададим им терм–множества, численные значения и функции принадлежности (табл. 1).

Таблица 1. – Экспертные оценки факторов «потенциала нападения»

Фактор (лингвистическая переменная)	Терм–множества	Функция принадлежности
k_1 = «общее затрачиваемое время»	K_1^0 = «за минуты»	$\mu(K_1^0) = (0; 0; 3)$
	K_1^1 = «за часы»	$\mu(K_1^1) = (0; 3; 6)$
	K_1^2 = «за дни»	$\mu(K_1^2) = (3; 6; 9)$
	K_1^3 = «за месяцы»	$\mu(K_1^3) = (6; 9; 9)$
k_2 = «компетентность нарушителя»	K_2^0 = «непрофессионал»	$\mu(K_2^0) = (0; 0; 3)$
	K_2^1 = «профессионал»	$\mu(K_2^1) = (0; 3; 6)$
	K_2^2= «эксперт»	$\mu(K_2^2) = (3; 6; 8)$
	K_2^3 = «группа экспертов»	$\mu(K_2^3) = (6; 8; 8)$
k_3 = «знание информационной системы»	K_3^0 = «общедоступная информация»	$\mu(K_3^0) = (0; 0; 3)$
	K_3^1 = «информация ограниченного доступа»	$\mu(K_3^1) = (0; 3; 7)$
	K_3^2 = «чувствительная информация»	$\mu(K_3^2) = (3; 7; 11)$
	K_3^3 = «критически важная информация»	$\mu(K_3^3) = (7; 11; 11)$
k_4 = «возможность доступа к информационной системе»	K_4^0 = «отсутствие необходимости в доступе/неограниченный доступ»	$\mu(K_4^0) = (0; 0; 1)$
	K_4^1 = «простой доступ»	$\mu(K_4^1) = (0; 1; 4)$
	K_4^2 = «умеренная возможность доступа»	$\mu(K_4^2) = (1; 4; 10)$
	K_4^3 = «затруднительный доступ»	$\mu(K_4^3) = (4; 10; 10)$
k_5 = «оборудование»	K_5^0 = «стандартное»	$\mu(K_4^0) = (0; 0; 4)$
	K_5^1 = «специализированное»	$\mu(K_4^1) = (0; 4; 7)$
	K_5^2 = «сделанное на заказ»	$\mu(K_4^2) = (4; 7; 9)$
	K_5^3 = «несколько видов на заказ оборудования»	$\mu(K_4^3) = (7; 9; 9)$

В дополнение можно сформулировать синтаксические правила для образования новых термов соответствующих промежуточным значениям.

Полученные числовые значения характеристик «потенциала нападения» суммируются:

$$K = K_1 + K_2 + K_3 + K_4 + K_5 \quad (1)$$

Введем теперь лингвистическую переменную k = «потенциал нападения». Множеством значений переменной k будет терм–множество $K = \{K^0; K^1; K^2; K^3; K^4\}$. Каждый терм из множества K является именем нечеткого подмножества на отрезке [0, 47]. Верхнее значение отрезка получено путем суммирования максимальных значений каждого показателя, составляющего «потенциал нападения» из табл. 2.

Таблица 2. – Диапазон значений «потенциала нападения»

Диапазон значений	Потенциал нападения (лингвистическая переменная)
0–9	K^0 = «базовый»
10–13	K^1 = «усиленный базовый»
14–19	K^2 = «умеренный»
20–24	K^3 = «высокий»
≥ 25	K^4 = «за пределами высокого»

Получаем четыре непересекающихся множества численных значений, соответствующих вербальным оценкам. Полученная сумма не будет иметь нечеткости. Значения лингвистической переменной «потенциал нападения» будут однозначно принадлежать определенному числовому промежутку. Функции принадлежности подмножеств терм–множества $K = \{K^0; K^1; K^2; K^3; K^4\}$ будут иметь прямоугольную форму. Их можно записать параметрами, рассматривая, как частный случай трапециевидных нечетких чисел: $\mu(K^0) = (0; 0; 9; 9)$, $\mu(K^1) = (10; 10; 13; 13)$, $\mu(K^2) = (14; 14; 19; 19)$, $\mu(K^3) = (20; 20; 24; 24)$, $\mu(K^4) = (25; 25; 47; 47)$.

Определение «потенциала нападения» имеет смысл если имеется мотивация нарушителя. Повышенная мотивация переводит «потенциал нападения» на следующий уровень. Соответственно для окончательной оценки «потенциала нападения» необходимо оценить влияющее воздействие мотивации (M).

Введем еще одну лингвистическую переменную m = «мотивация нарушителя для реализации угроз». В качестве универсального множества для этой переменной примем отрезок [0; 1]. Множеством значений этой переменной будет терм–множество $M = \{M_1; M_2; M_3\}$ соответствующее следующим именам нечетких подмножеств: M_1 – «мотивация отсутствует»; M_2 – «базовая мотивация»; M_3 – «повышенная мотивация».

С учетом того, что эксперт в определенных случаях может с полной уверенностью дать заключение о мотивации, а в некоторых случаях полной уверенности не будет, то уместно рассматривать эти нечеткие подмножества как трапециевидные нечеткие числа.

Составим функции принадлежности каждого терма и сведем в табл. 3.

Таблица 3. – Функции принадлежности термов множества M_k

Терм M_k	Функция принадлежности нечеткого множества M_k
M_1 = «мотивация отсутствует» $M_1 \in [0; 0{,}4]$	$\mu_1(m) = \begin{cases} 1, \textit{ если } 0 \le m \le 0{,}2 \\ 5(0{,}4 - m), \textit{ если } 0{,}2 < m \le 0{,}4 \end{cases}$
M_2 = «базовая мотивация» $M_2 \in (0{,}2; 0{,}8]$	$\mu_2(m) = \begin{cases} 5(m - 0{,}2), \textit{ если } 0{,}2 < m \le 0{,}4 \\ 1, \textit{ если } 0{,}4 < m \le 0{,}6 \\ 5(0{,}8 - m), \textit{ если } 0{,}6 < m \le 0{,}8 \end{cases}$
M_3 = «повышенная мотивация» $M_3 \in (0{,}6; 1]$	$\mu_3(m) = \begin{cases} 5(m - 0{,}6), \textit{ если } 0{,}6 \le m < 0{,}8 \\ 1, \textit{ если } 0{,}8 \le m \le 1 \end{cases}$

Для краткости записи в формулах функций опущены интервалы, на которых они принимают нулевые значения.

Теперь с учетом влияния мотивации нарушителя для реализации угроз, оценку «потенциала нападения» можно производить матричным способом. Матрица соотнесения оценочных значений потенциала и мотивации будет выглядеть как представлено в табл. 4.

Таблица 4. – «Потенциал нападения с учетом мотивации нарушителя

Значение потенциала нападения	Мотивация нарушителя для реализации угроз		
	Мотивация отсутствует	Базовая мотивация	Повышенная мотивация
0–9	Недостаточен	Базовый (K^0)	Усиленный базовый (K^1)
10–13	Недостаточен	Усиленный базовый (K^1)	Умеренный (K^2)
14–19	Недостаточен	Умеренный (K^2)	Высокий (K^3)
20–24	Недостаточен	Высокий (K^3)	За пределами высокого (K^4)
≥ 25	Недостаточен	За пределами высокого (K^4)	За пределами высокого (K^4)

На основании матрицы можно сформулировать ряд логико–лингвистических продукционных правил вывода:

1. ЕСЛИ «мотивация отсутствует», ТО «потенциал недостаточен для реализации угрозы безопасности» при любом численном значении;

2. ЕСЛИ «базовая мотивация» И численное значение потенциала меньше 10, ТО «потенциал базовый»;

3. ЕСЛИ «базовая мотивация» И численное значение потенциала от 10 до 13, ТО «усиленный базовый потенциал»;

4. ЕСЛИ «базовая мотивация» И численное значение потенциала от 14 до 19, ТО «умеренный потенциал»;

5. ЕСЛИ «базовая мотивация» И численное значение потенциала от 20 до 24, ТО «высокий потенциал»;

6. ЕСЛИ «базовая мотивация» И численное значение потенциала 25 и больше, ТО «потенциал за пределами высокого»;

7. ЕСЛИ «повышенная мотивация» И численное значение потенциала меньше 10, ТО «усиленный базовый потенциал»;

8. ЕСЛИ «повышенная мотивация» И численное значение потенциала от 10 до 13, ТО «умеренный потенциал»;

9. ЕСЛИ «повышенная мотивация» И численное значение потенциала от 14 до 19, ТО «высокий потенциал»;

10. ЕСЛИ «повышенная мотивация» И численное значение потенциала 20 и больше, ТО «потенциал за пределами высокого».

После применения вышеприведенных продукционных правил 7–10 лингвистическим переменным K^0; K^1; K^2; K^3; K^4 присваиваются значения, соответствующие середине диапазона (табл. 3): $K^0 = 4{,}5$; $K^1 = 11{,}5$; $K^2 = 21{,}5$; $K^3 = 22$; $K^4 = 36$. Для правил 2–6 берутся значения, соответствующие лингвистическим переменным.

Предложенный метод представления экспертных оценок при моделировании нарушителя на основе нечетких множеств легко реализуется в виде программного обеспечения. Автоматизация данного процесса позволит снизить трудоемкость и экспертную субъективность.

Список использованных источников

1. Власенко А.В., Жук Р.В. Анализ характеристик определения нарушителя при моделировании угроз информационной безопасности в информационных системах персональных данных // Научные труды КубГТУ. – 2016. – № 16.

2. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие. – СПб: Университет ИТМО, 2015. – 93с.

3. Нечунаев В.М. Оценка рисков информационной безопасности. // Доклады ТУСУРа, № 1 (19), часть 2, июнь 2009. – С. 51–53.

4. Булдакова Т. И. Миков Д. А. Реализация методики оценки рисков информационной безопасности в среде MATLAB. // Вопросы кибербезопасности №4(12) – 2015. С. 53–61.

5. ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation