МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ

УДК 004.056.53

ОЦЕНКА ВОЗМОЖНОСТИ ВОЗНИКНОВЕНИЯ УГРОЗЫ 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, Irkutsk

Определение риска информационной безопасности предполагает оценку вероятности возникновения угрозы, производимую экспертным методом. С целью формализации этого процесса предлагается применение математических методов нечеткой логики, для последующей автоматизации и исключения субъективности.

Риск-ориентированный подход к оценке угроз информационной безопасности предполагает обязательную оценку вероятности негативного события и его последствий [1]. В стандарте обозначено, что риск измеряется исходя из комбинации последствий, вытекающих из нежелательного события и вероятности возникновения события. Установление значения риска может быть качественным, количественным или комбинированным, в зависимости от обстоятельств. Рекомендуется использовать качественные значения для получения общих сведений об уровне риска и затем переходить к количественным оценкам, как к более детальным. Сначала проводятся качественные оценки последствий (ценности активов) и степени вероятности возникновения угрозы затем им в соответствие ставятся численные значения по заранее определенной шкале. Количественное значение риска вычисляется путем перемножения значения последствий на значение вероятности.

Для степени вероятности возникновения угрозы напрашивается трактовка ее с математической точки зрения. Так как угрозы являются наблюдаемыми событиями, то и вероятность их проявления – это число, около которого группируются значения частоты данного события в различных сериях большого числа испытаний. Значит, степень вероятности возникновения угрозы должна иметь численное выражение, применение качественных оценок является не совсем корректным в математической трактовке. Получить количественную оценку вероятности реализации можно на основе использования статистических данных, если они есть.

Математически такой подход является наиболее корректным, когда есть возможность получить численные значения вероятности на основе статистических данных, то эти численные значения и должны использоваться. Однако не всегда корректные статистические данные о частоте реализации угроз безопасности информации имеются в распоряжении. Можно использовать статистику однотипной информационной системы, однако любая информационная система охватывающая большинство процессов деятельности организации является уникальной. Даже если применяются тиражируемые программные решения, всегда найдутся отличия в аппаратном обеспечении, сетевой инфраструктуре, количестве субъектов доступа, а соответственно и потенциальных нарушителей и т.д.

Система менеджмента риска предлагает альтернативный вариант с использованием не вероятности, а возможности возникновения угроз безопасности информации [2] определяемой в качественных экспертных характеристиках. Вербальные экспертные оценки хорошо формализуются с помощью математического аппарата теории нечетких множеств.

Предлагается решение задачи оценки степени возможности возникновения угроз информационной безопасности в условиях отсутствия статистических данных о частоте их реализации с применением нечеткой логики.

Рассмотрим подробнее возможность возникновения угрозы (Y_j), а именно каким образом эксперт получает качественное значение этого параметра. Y_j — является функцией двух аргументов и

оценивается сопоставлением «уровня защищенности» (Y_1) информационной системы и «потенциала нападения» (Y_2):

$$Y_j = [Y_1; Y_2] \quad (1)$$

Значение возможности возникновения угрозы имеет прямую зависимость от «потенциала нападения» и обратную от «уровня защищенности». Можно предположить, что оба аргумента имеют равный вес для значения функции.

Все вышесказанное можно записать в математической интерпретации:

$$Y_j = (1 - Y_1) \cdot Y_2 . \quad (2)$$

Оба показателя должны быть нормированы.

Основным критерием оценки «уровня защищенности» (Y_1) информационной системы является возможность оперативного принятия мер по нейтрализации новых идентифицированных угроз. Для оценки оперативности можно принять подход, предлагавшийся в одном проекте методического документа ФСТЭК России [3]. Если защитные меры могут быть приняты «за минуты», то получаем высокий уровень, если за «за часы», то средний уровень. Низкий уровень характеризуется невозможностью оперативного принятия защитных мер, без уточнения порядка временного интервала. Если рассматривать возможность получения количественных оценок параметра (Y_1), то это возможно только для высокого уровня. Принятие мер «за минуты» подразумевает меньше часа, таким образом в абсолютных единицах это интервал $Y_1^h \in [0; 60)$. Гораздо сложнее определиться со средним уровнем, как понимать «за часы». Понятно, что нижняя граница начинается с 60-ти минут, а вот чем ограничивается верхняя граница. Это меньше суток, 24 часа? Или это меньше 8-ми часов исходя из продолжительности рабочего дня? Еще хуже ситуация для низкого уровня с таким размытым понятием, как принятие мер с высокой оперативностью.

Наверняка для разных объектов, в зависимости от вида деятельности, деловых процессов и значимости информации будет разный временной интервал, который организация может себе позволить для принятия мер по нейтрализации угроз. Наиболее приемлемым здесь будет устанавливать верхнюю границу среднего «уровня защищенности» t исходя из специфики объекта информатизации. В одном случае оперативное принятие мер «за часы» будет не более 2-х часов, в другом не более 8-ми. Тогда интервалы численных значений будут выглядеть следующим образом: $Y_1^h \in [0; 60)$ для высокого уровня, $Y_1^m \in [60; t]$ для среднего уровня и $Y_1^l \in (t; \infty)$ для низкого уровня эксплуатационной защищенности. Делаем вывод, что уровень эксплуатационной защищенности в принципе можно оценить количественно. Однако понятно, что это будут нечеткие интервалы значений, границы их будут размыты.

«Потенциал нападения» (Y_2) является вторым аргументом функции определения возможности возникновения угрозы. Заключение о нем эксперт делает на основании анализа пяти факторов [4]. Значение его можно представить в виде лингвистической переменной y_2 = «потенциал нападения» с множеством значений Y_2 = {K^0 = «базовый», K^1 = «усиленный базовый», K^2 = «умеренный», K^3 = «высокий», K^4 = «за пределами высокого»}. Функции принадлежности: $\mu(K^0)$ = (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). Подробно об этом представлено в работе [5].

В силу вышесказанного применение методов математической статистики и теории вероятности будет не корректным, так как исходные данные не обладают определенной точностью и достоверностью.

Рассмотрим оценку значения лингвистической переменной y = «возможность возникновения угрозы», которая определена на отрезке [0; 1]. Множеством значений переменной y является терм множество Y = {Y^1, Y^2, Y^3}, где Y^1 = «низкая возможность», Y^2 = «средняя возможность», Y^3 = «высокая возможность».

Каждый терм множества Y_j будем рассматривать, как нечеткое число с трапециевидной функцией принадлежности: $\mu(Y^1) = (0; 0; 0{,}2; 0{,}4)$, $\mu(Y^2) = (0{,}2; 0{,}4; 0{,}6; 0{,}8)$, $\mu(Y^3) = (0{,}6; 0{,}8; 1; 1)$.

Вводим еще одну лингвистическую переменную y_1 = «уровень защищенности». Множеством значений переменной y_1 является терм-множество Y_1 = { Y_1^l = «низкий уровень»; Y_1^m = «средний уровень»; Y_1^h = «высокий уровень»}. Приведенные выше интервалы значений для термов Y_1 не совсем корректно использовать, как четкие множества. Границы их будут размыты. Явно, что для одного эксперта понятие «за минуты» это не более часа, а для другого не более получаса. Такая же размытость будет наблюдаться на границе среднего и высокого уровней, потому что t можно установить только с неопределенностью, например, «около трех часов». Исходя из сказанного, значения термов лингвистической переменной y_1 = «уровень защищенности» будем рассматривать, как трапециевидные нечеткие числа. Универсальным множеством будет числовой промежуток [0; ∞) и за единицу измерений примем 1 час. Зададим параметрическим методом функции принадлежности подмножествам множества Y_1: $\mu\left(Y_1^l\right) = (0; 0; 0{,}5; 1)$, $\mu\left(Y_1^m\right) = (0{,}5; 1; (t-1); t)$, $\mu\left(Y_1^h\right) = ((t-1); t; \infty; \infty)$.

Если обратиться к формуле (2), то там в качестве множителя выступает нечеткое число $(1 - Y_1)$ при условии, что Y_1 нормирован. Произведем нормирование по t и найдем параметры функций принадлежности $(1 - Y_{1норм})$:

$$\mu\left(1 - Y_{1норм}^h\right) = \left(-\infty; -\infty; 0; 1/t\right);$$

$$\mu\left(1 - Y_{1норм}^m\right) = \left(0; 1/t; (1-1/t); (1-1/2t)\right);$$

$$\mu\left(1 - Y_{1норм}^l\right) = \left((1-1/t); (1-1/2t); 1; 1\right).$$

Значения от $-\infty$ до 0 для $\mu\left(1 - Y_{1норм}^h\right) = \left(-\infty; -\infty; 0; 1/t\right)$ мы отбрасываем, как не представляющие интереса.

Далее нам необходимо перейти от значений показателей $(1 - Y_1)$ и Y_2 к лингвистическим переменным Y_j. Составим матрицу определения интервалов «возможности возникновения угрозы».

Таблица – Определение интервалов возможности возникновения угроз

Потенциал нарушителя (Y_2)	Уровень защищенности (Y_1)		
	Высокий	**Средний**	**Низкий**
K^0 = «базовый»	Низкая $\left(1 - Y_1^h\right) \cdot K^0$	Низкая $\left(1 - Y_1^m\right) \cdot K^0$	Средняя $\left(1 - Y_1^l\right) \cdot K^0$
K^1 = «усиленный базовый»	Низкая $\left(1 - Y_1^h\right) \cdot K^1$	Средняя $\left(1 - Y_1^m\right) \cdot K^1$	Средняя $\left(1 - Y_1^l\right) \cdot K^1$
K^2 = «умеренный»	Средняя $\left(1 - Y_1^h\right) \cdot K^2$	Средняя $\left(1 - Y_1^m\right) \cdot K^2$	Высокая $\left(1 - Y_1^l\right) \cdot K^2$
K^3 = «высокий»	Средняя $\left(1 - Y_1^h\right) \cdot K^3$	Высокая $\left(1 - Y_1^m\right) \cdot K^3$	Высокая $\left(1 - Y_1^l\right) \cdot K^3$
K^4 = «за пределами высокого»	Высокая $\left(1 - Y_1^h\right) \cdot K^4$	Высокая $\left(1 - Y_1^m\right) \cdot K^4$	Высокая $\left(1 - Y_1^l\right) \cdot K^4$

Далее находим произведения нечетких множеств согласно табл. 1, затем объединяем полученные в результате множества по соответствию значениям терм-множества $Y = \{Y^1, Y^2, Y^3\}$. В результате получим прообразы $f^{-1}(Y^1)$, $f^{-1}(Y^2)$ и $f^{-1}(Y^3)$, которые условно можно обозначить как $B = \{B_1, B_2,$

$B_3\}$. Прообразы нужно отобразить на множество значений лингвистической переменной y = «возможность возникновения угрозы»: $B_1 \to Y^1$, $B_2 \to Y^2$, $B_3 \to Y^3$.

Другим альтернативным способом оценки y = «возможность реализации угрозы», является формирование продукционных правил нечеткого вывода на основании матрицы представленной в табл. 1. Такой подход позволит избежать трудоемких арифметических операций с нечеткими множествами. Сформулируем данные правила.

1. **ЕСЛИ** «потенциал нападения» базовый **И** «уровень защищенности» высокий **ИЛИ** средний, **ТО** «возможность возникновения угрозы» низкая.

2. **ЕСЛИ** «потенциал нападения» усиленный базовый **И** «уровень защищенности» высокий, **ТО** «возможность возникновения угрозы» низкая.

3. **ЕСЛИ** «потенциал нападения» базовый **И** «уровень защищенности» низкий, **ТО** «возможность возникновения угрозы» средняя.

4. **ЕСЛИ** «потенциал нападения» усиленный базовый **И** «уровень защищенности» средний **ИЛИ** низкий, **ТО** «возможность возникновения угрозы» средняя.

5. **ЕСЛИ** «потенциал нападения» умеренный **И** «уровень защищенности» высокий **ИЛИ** средний, **ТО** «возможность возникновения угрозы» средняя.

6. **ЕСЛИ** «потенциал нападения» высокий **И** «уровень защищенности» высокий, **ТО** «возможность возникновения угрозы» средняя.

7. **ЕСЛИ** «потенциал нападения» умеренный **И** «уровень защищенности» низкий, **ТО** «возможность возникновения угрозы» высокая.

8. **ЕСЛИ** «потенциал нападения» высокий **И** «уровень защищенности» средний **ИЛИ** низкий, **ТО** «возможность возникновения угрозы» высокая.

9. **ЕСЛИ** «потенциал нарушителя» за пределами высокого **И** «уровень защищенности» высокий **ИЛИ** средний **ИЛИ** низкий, **ТО** «возможность реализации угрозы» высокая.

Вариант вывода решения на основе продукционных правил нечеткой логики явно проще для программной реализации, чем на основе арифметических операций. Какой же из этих вариантов дает наиболее объективный результат оценки, можно будет судить только после сравнения реализации в виде программного обеспечения.

Список использованных источников

1. ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management.

2. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» РС БР ИББС-2.2-2009 (приняты и введены в действие Распоряжением Банка России от 11.11.2009 N Р-1190).

3. «Методика определения угроз безопасности информации в информационных системах» [Электронный ресурс] / ФСТЭК России. Проект. – Режим доступа: http://fstec.ru/component/attachments/download/812 (дата обращения 20.01.2021).

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

5. Бусько М.М. Модель нарушителя информационной безопасности на основе нечетких множеств // Инжиниринг: теория и практика: материалы I международной заочной научно-практической конференции, УО «Полесский государственный университет», г. Пинск, 26 марта 2021 г. / Министерство образования Республики Беларусь [и др.]; редкол.: В.И. Дунай [и др.]. – Пинск: ПолесГУ, 2021. – С. 7-11.