М. В. Тимонин, В. С. Лаврентьев

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ К МОДЕЛИРОВАНИЮ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОСНОВАННЫХ НА ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ И БАЙЕСОВЫХ СЕТЯХ

Традиционным подходом к моделированию риска информационной безопасности является использование вероятностных методов, в частности байесовых сетей.

Байесова сеть представляет собой направленный ациклический граф, основными целями которого являются:

1. удобный способ описания составляющих исследуемой проблематики,
2. экономичное представление многомерных распределений,
3. построение следствий на основе наблюдений [3].

Фактически, при разложении риска на компоненты, организованные в виде графа, мы получаем многомерное распределение на n дихотомических переменных. Для полного описания этого распределения потребовалась бы таблица с 2^n записями. Однако это число можно значительно уменьшить, если принять во внимание, что каждая переменная непосредственно зависит лишь от небольшого числа элементов. Использование направленных ациклических графов позволяет эффективно проиллюстрировать подобный подход.

Итак, предположим, что мы рассматриваем распределение P на n дискретных переменных X1,...,Xn. Мы можем представить P как произведение n условных вероятностей:

$$P(x_1,...,x_n)=\prod P(x_j \mid x_1,...,x_{j-1}).$$

Предположим теперь, что условная вероятность переменной X_j зависит не от всех предшествующих ей вершин, а только от небольшого подмножества PA_j.

Определение 1 [4]:

Пусть $V = \{X_1, ..., X_n\}$– упорядоченное множество переменных, а $P(v)$ – совместное распределение на этих переменных. Марковскими родителями вершины X_j называется множество переменных PA_j – минимальное множество предшественников X_j , которое представляет X_j независимым от всех остальных предшественников. Иными словами,

$$PA_j \subset \{X_1, ..., X_{j-1}\} : P(x_j \mid x_1, ..., x_{j-1}) = P(x_j \mid \rho_{aj}).$$

И не существует такого подмножества множества PA_j, для которого равенство выполнялось бы.

Байесовой сетью называется направленный ациклический граф, в котором каждая стрелка от X_i к X_j , символизирует то, что X_i является марковским родителем X_j .

Рассмотрим теперь, каким образом мы можем смоделировать риск с помощью байесовой сети. К примеру, существует некое понятие A, которое мы логически раскладываем на три компонента B, C и D (рис. 1). Каждая из переменных является дихотомической, т. е. принимает два значения, к примеру, для A — a и $\neg a$. В байесовском формализме данная структура будет выглядеть следующим образом (Рис. 1).

Таким образом, вершины B, C и D являются марковскими родителями вершины A.

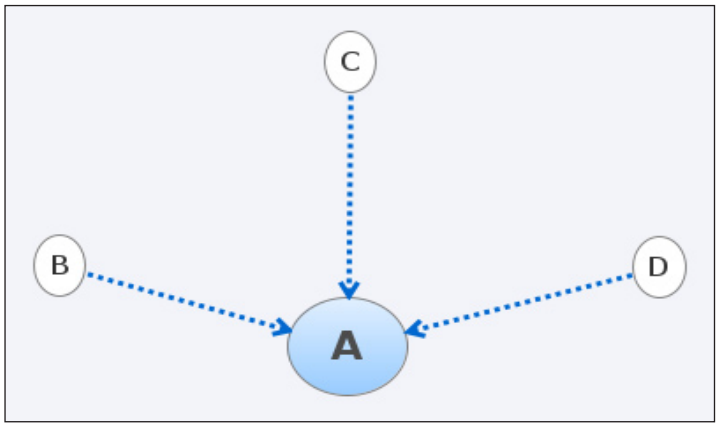

Рис. 1. Моделирование трех независимых компонентов с помощью теории вероятностей

Для выражения связи между переменными A и B, C, D создается таблица условных вероятностей, содержащая все сочетания значений B, C и D и соответствующие условные вероятности значений a и $\neg a$.

	a	$\neg a$
$(\neg b, \neg c, \neg d)$	0	1
$(b, \neg c, \neg d)$	0.6	0.4
$(\neg b, c, \neg d)$	0.2	0.2
$(\neg b, \neg c, d)$	0.2	0.2
$(b, c, \neg d)$	0.7	0.9
$(b, \neg c, d)$	0.9	0.1
$(\neg b, c, d)$	0.2	0.2
(b, c, d)	1	0

Фактически условные вероятности в данном подходе играют роль весов в логических высказываниях типа «A наступит с такой-то вероятностью, если произошло...». Иными словами, мы задаем, насколько вероятным является событие A при выполнении определенной комбинации событий B, C и D. Следует обратить внимание на схожесть данной концепции с понятием нечеткой меры $м$. Для определения значения интересующей нас переменной используется следующая формула:

$$P(A) = \sum_{i,j,k,} P(A \mid B_i, C_j, D_k)P(B, C, D) = \sum_{i,j,k,} P(A \mid B_i, C_j, D_k)P(B_i)P(C_j)P(D_k).$$

Мы можем рассматривать процесс расчета интересующей нас переменной на основе условных вероятностей, связывающих переменную с сочетаниями компонентов, и априорных вероятностей собственно компонентов как агрегацию наших знаний о системе. Данные вероятности рассматриваются, естественно, не в частотном смысле, а в субъективном, т. е. отражают уверенность в том, насколько тот или иной компонент соответствует желаемому, иными словами, в рамках контекста тот или иной элемент защиты присутствует, правильно функционирует и надежен.

Оператор обладает достаточно большой выразительной силой, в частности, выполняются свойства 1–4 и 6, 7, 8, 10 [1]. (Монотонность не выполняется в общем случае, но может быть сформулирована как ограничение.) Однако не выполняются свойства 5 (идемпотентность) и 9

(компенсируемость). В контексте решаемой задачи несоблюдение данных требований вызывает некоторые проблемы. В качестве иллюстрации рассмотрим пример, приведенный выше.

Таблица определяет веса отдельных переменных и их сочетаний в общей сумме. Так, переменная B оказывает более сильное влияние на A, нежели C и D. Далее, переменные B и C усиливают друг друга ($P(a \mid b, c, \neg d) > P(a \mid b, \neg c, \neg d) + P(a \mid \neg b, c, \neg d)$), B и D являются в некоторой степени взаимозаменяемыми ($P(a \mid b, \neg c, d) < P(a \mid b, \neg c, \neg d) + P(a \mid \neg b, \neg c, d)$), C и D являются полностью взаимозаменяемыми ($P(a \mid \neg b, c, d) = P(a \mid \neg b, c, \neg d) = P(a \mid \neg b, \neg c, d)$). Невыполнение компонентов B, C и D ведет к невыполнению A($P(a \mid \neg b, \neg c, \neg d) = 0$). Присутствие B, C и D является достаточным для выполнения A($P(a \mid b, c, d) = 1$).

Таким образом, рассматриваемый случай является общим примером, не находящимся ни в одном из крайних логических положений (AND и OR). Положим теперь P(b) = P(c) = P(d) = 0.9. Агрегация значений для расчета P(a) дает

$$P(A) = \sum_{i,j,k,} P(A \mid B_i, C_j, D_k) P(B_i) P(C_j) P(D_k).$$

Агрегированное значение, таким образом, находится ниже min(B,C,D), что в данном контексте (требование компенсируемости не должно быть нарушено) является неверным.

Сравнение подходов, основанных на интеграле Шоке и теореме Байеса, в рамках решаемой задачи

Как становится ясным из сказанного выше, механизмы теории вероятностей и подхода, основанного на нечетких множествах, схожи. Рассмотрим два предельных примера, позволяющих подчеркнуть разницу между ними в контексте исследуемой проблемы. В качестве структуры модели будет использоваться приведенные ранее граф (3 родительские вершины и одна дочерняя).

Рассмотрим 2 предельных случая:

• AND — система защиты актива, состоит из трех компонентов. Взлом каждого из элементов защиты приведет к компрометации системы.

• OR — система обнаружения атак, включает три датчика. Срабатывание любого датчика приведет к активации тревоги.

AND		OR	
	$м(\varnothing) = 0$		$м(\varnothing) = 0$
	$м(a_1) = 0$		$м(a_1) = 1$
	$м(a_2) = 0$		$м(a_2) = 1$
	$м(a_3) = 0$		$м(a_3) = 1$
	$м(a_1, a_2) = 0$		$м(a_1, a_2) = 1$
	$м(a_1, a_3) = 0$		$м(a_1, a_3) = 1$
	$м(a_2, a_3) = 0$		$м(a_2, a_3) = 1$
	$м(a_1, a_2, a_3) = 1$		$м(a_1, a_2, a_3) = 1$

Зафиксируем теперь два из трех критериев на 0.5 и посмотрим, как будет зависеть значение агрегируемой переменной от третьего компонента. Графики зависимости агрегированного значения от значения переменной изображены на рис. 2.

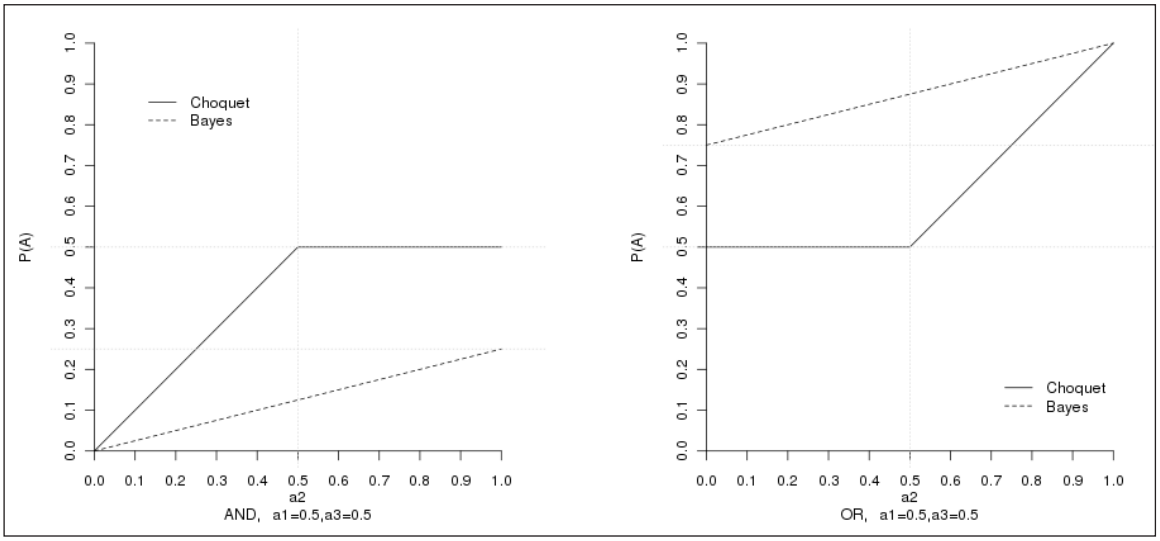

Рис. 2. Сравнение AND и OR в моделях на основе нечетких множеств и теории вероятностей

Как мы видим, в первом случае агрегированное значение, рассчитанное с помощью интеграла Шоке, демонстрирует более позитивную оценку, ограниченную сверху значением 0.5, а во втором — более негативную, ограниченную снизу значением 0.5. С чем связана разница в результатах, полученных с помощью двух подходов, и как следует трактовать данное расхождение?

Причиной является различная семантическая трактовка значений. В случае теории вероятностей 0.5 означает, что механизм защиты остановит (датчик уловит) 50 % атак. Подобная оценка была бы верна при условии равномерного частотного распределения атак по качеству исполнения и равномерного же распределения вектора атаки. Иными словами, число экспертных, хорошо подготовленных атак считается равным числу неквалифицированных попыток вторжения, а атакуемый механизм выбирается случайно, с вероятностью 1/3. Поэтому увеличение качества одного механизма из трех ведет к линейному росту общей защищенности системы.

В случае интеграла Шоке значение критерия выражает его качество. Иными словами, 0.5 будет означать, что механизм способен остановить (датчик способен детектировать) атаки определенного уровня по шкале [0,1]. Напомним также, что расценивать атакующего в качестве стохастического генератора не вполне верно, успешная атака будет гарантированно проведена через самое слабое звено в защите системы. Таким образом, даже при увеличении качества одного из механизмов (например, введения более сильной системы шифрования) общий уровень защиты должен быть ограничен сверху слабейшим элементом системы (к примеру, легко подбираемыми паролями) и равняться ему. Таким образом, можно с уверенностью заявить, что использование методики, основанной на интеграле Шоке, предпочтительно для моделирования в рамках исследуемой проблемы.

Достаточно любопытным является также следующий факт. Рассмотрим некие значения нечеткой меры и критериев, не носящих предельный характер, как в приведенных выше примерах. Семантический смысл приведенной ниже нечеткой меры таков: компоненты 2 и 3 важнее, чем 1, сочетание 1 и 2 слабее, чем 1 и 3, при этом в обоих случаях компоненты усиливают друг друга (супераддитивность), сочетание 2 и 3 лишь незначительно сильнее, чем присутствие 2 и 3 по отдельности (субаддитивность) [1].

$м\ (\varnothing) = 0$
$м\ (a_1) = 0.2$
$м\ (a_2) = 0.4$
$м\ (a_3) = 0.4$
$м\ (a_1, a_2) = 0.7$
$м\ (a_1, a_3) = 0.8$
$м\ (a_2, a_3) = 0.5$
$м\ (a_1, a_2, a_3) = 1$

Вновь зафиксируем компоненты 1 и 3 и построим зависимость общего значения от величины компонента 2. На рис. 3 видно, что интеграл Шоке является нелинейной функцией, имеющей излом в точках, соответствующих значениям критериев, т. е. отражает взаимодействие между компонентами. В то же время агрегация с помощью формализма теории вероятностей является строго линейной аппроксимацией моделируемой ситуации.

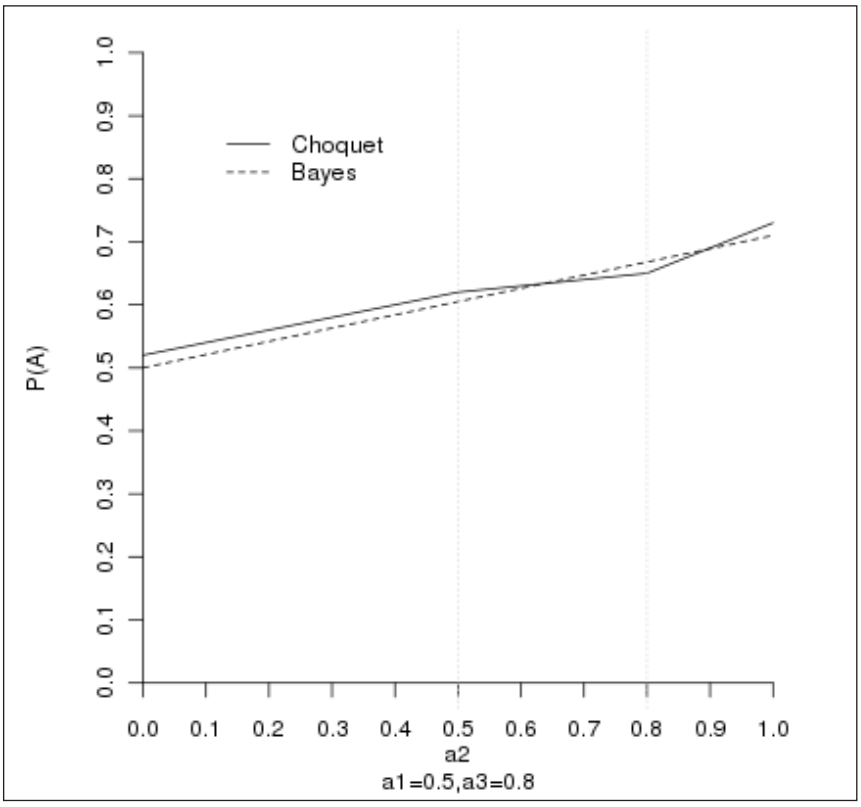

Рис. 3. Моделирование общего случая

Выводы

Использование теории нечеткой меры при моделировании риска информационной безопасности обладает весомыми преимуществами в сравнении с классическим вероятностным подходом. Высокая семантическая выразительность и легкость использования и трактования позволяют широко применять метод для решения практических задач. К достоинствам подхода следует отнести также и достаточно развитые механизмы, облегчающие процесс моделирования в рассматриваемой проблематике. Это и принципы ветирования и достаточности [1], и понятие k-аддитивности [5], и индексы взаимодействия между критериями — величина Шепли [1].

СПИСОК ЛИТЕРАТУРЫ:

1. *Тимонин М. В., Лаврентьев В. С.* Использование теории нечеткой меры для агрегации составляющих риска информационной безопасности // Безопасность информационных технологий. 2009. № 4. С. 31–35.
2. *Тимонин М. В., Лаврентьев В. С.* Пример моделирования риска информационной безопасности с помощью теории нечеткой меры // Безопасность информационных технологий. 2010. № 1. С. 30–35.
3. *Pearl J.* Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Morgan Kaufmann, San Mateo, CA, 1988.
4. *Pearl J.* Causality: Models, Reasoning, and Inference. Cambridge University Press, 2000.
5. *Grabisch M.* K-order Additive Fuzzy Measures // 6th Int. Conf. on Information Processing and Management of Uncertainty in Knowledge-Based Systems (IPMU). Granada, Spain, 1996. P. 1345–1350.