Знания-Онтологии-Теории (ЗОНТ-09)

Оценка рисков информационной безопасности на основе нечеткой логики

Д.Ж. Сатыбалдина, А.А. Шарипбаев

Евразийский национальный университет им. Л.Н.Гумилева, ул. Мунайтпасова, д. 5, г.Астана, 010000, Республика Казахстан

dinasaty@gmail.com, sharalt@mail.ru

Аннотация. *В работе описывается методика анализа информационной безопасности с помощью инструмента искусственного интеллекта – иерархического нечеткого логического вывода. Предложенный метод оценки уровня защищенности информации позволяет перейти к количественным процедурам оценки опасности угроз безопасности информации, учесть сравнительную важность для организации или пользователя того или иного вида ущерба и характеристики динамики реализации различных угроз, а также состав и характеристики применяемых мер и средств защиты и на этой основе оценивать их эффективность.*

Ключевые слова: информационная безопасность, риски, нечеткая логика, нечеткое множество, функция принадлежности, лингвистическая переменная

1 Введение

Информационные технологии все шире применяются в качестве инструмента ведения бизнеса. В связи с ростом зависимости организаций от информационных систем и сервисов происходит резкое увеличение рисков, связанных с недостаточным уровнем обеспечения безопасности получения, хранения и переработки информации. Понятие риска становится краеугольным как для бизнеса, так и для системы организации информационной безопасности. Возникает острая необходимость использования международных стандартов построения информационных систем и систем информационной безопасности (BASEL II, SOX, Cobit, BS 17799, ISO 15408, NIST 80030, SAC, COSO, SAS 55/78 ITIL и др.), которые суть не что иное, как собранные в одном документе передовые практики построения подобных систем.

В соответствие с этими практиками управление информационными рисками любой компании предполагает следующее. Во-первых, определение основных целей и задач защиты информационных активов компании. Во-вторых, создание эффективной системы оценки и управления информационными рисками. В-третьих, расчет совокупности детализированных не только качественных, но и количественных оценок рисков, адекватных заявленным целям бизнеса. В-четвертых, применение специального инструментария оценивания и управления рисками.

Ключевым является выбор методики оценки рисков. Многие документы содержат рекомендации по выбору методики (например, ГОСТ Р ИСО/МЭК 13335-3-2007), в них предлагаются различные способы сопоставления возможных последствий реализации угрозы с вероятностью ее реализации и получения соответствующих выводов. В зависимости от «математизации» этой процедуры сопоставления и выводов методики делят на качественные, полуколичественные и количественные. Адекватность применения этих методов по отношению к объектам информационной инфраструктуры требует как минимум дополнительного обоснования. Современные методы оценки рисков имеют ряд ограничений. Вместе с тем сам рискориентированный подход к управлению информационной безопасностью (ИБ) представляется перспективным, в связи, с чем совершенствовать методы оценки рисков в направлении преодоления тех ограничений и недостатков, которыми они обладают в настоящее время.

В данной работе представлен механизм получения оценок рисков ИБ на основе нечеткой логики, который позволяет заменить приближенные табличные методы оценки рисков современным математическим методом, адекватным рассматриваемой задаче.

2 Теоретические проблемы

2.1 Постановка задачи

Оценка рисков (risk assessment) – первый этап в управлении системы ИБ, предназначенный для идентификации источников рисков и определения его уровня значимости. Оценку разбивают на анализ рисков и оценивание рисков.

В рамках анализа проводится инвентаризация и категоризация защищаемых ресурсов, выясняются нормативные, технические, договорные требования к ресурсам в сфере ИБ, а затем с учетом этих требований определяется стоимость ресурсов. В стоимость входят все потенциальные затраты, связанные с возможной компрометацией защищаемых ресурсов. Следующим этапом анализа рисков является составление перечня значимых угроз и уязвимостей для каждого ресурса, а затем вычисляется вероятность их реализации. Международные стандарты допускают двоякое толкование понятия угрозы ИБ: как условие реализации уязвимости ресурса (в этом случае уязвимости и угрозы идентифицируются отдельно) и как общее потенциальное событие, способное привести к компрометации ресурса (когда наличие возможности реализации уязвимости и есть угроза). Не возбраняется разделение угроз ИБ на угрозы целостности, доступности и конфиденциальности.

Оценивание риска проводится путем его вычисления и сопоставления с заданной шкалой. Вычисление риска состоит в умножении вероятности компрометации ресурса на значение величины ущерба, связанного с его компрометацией. Сопоставление риска выполняется с целью упрощения процесса использования на практике точечных значений риска.

Международные стандарты допускают использование как количественных, так и качественных методов оценки рисков. Оцениваются уровни стоимости идентифицированного ресурса по пятибалльной шкале: «незначительный», «низкий», «средний», «высокий», «очень высокий». Оцениваются уровни вероятности угрозы по трехбалльной шкале: «низкий», «средний», «высокий». Оцениваются уровни вероятности уязвимости: «низкий», «средний», «высокий». По заданной таблице рассчитываются уровни риска. Проводится ранжирование инцидентов по уровню риска.

Для оценки рисков информационной системы организации защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов организации.

Владельцу информационной системы требуется сначала описать архитектуру своей сети:

- все ресурсы, на которых хранится ценная информация;
- все сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации по трем видам угроз;
- бизнес-процессы и информация, которая в них участвует;
- группы пользователей, имеющих доступ к ценной информации;
- класс группы пользователей;
- доступ группы пользователей к информации;
- характеристики этого доступа (вид и права);
- средства защиты информации;
- средства защиты рабочего места группы пользователей.

Механизм оценивания рисков на основе нечеткой логики по существу является экспертной системой, в которой базу знаний составляют правила, отражающие логику взаимосвязи входных величин и риска. В простейшем случае это «табличная» логика, в общем случае более сложная логика, отражающая реальные взаимосвязи, которые могут быть формализованы с помощью продукционных правил вида «Если ..., то…». Кроме того, механизм нечеткой логики требует формирования оценок ключевых параметров и представления их в виде нечетких переменных. При этом необходимо учитывать множество источников информации и неопределенность самой информации.

Математическая теория нечетких множеств, предложенная Л.Заде, позволяет описывать нечеткие понятия и знания, оперировать этими знаниями и делать нечеткие выводы [1].

В большинстве случаев показатели, оцениваемые при анализе рисков, однозначно нормировать невозможно. Ряд параметров оказывается недоступным для точного измерения, и тогда в его оценке неизбежно появляется субъективный компонент, выражаемый нечеткими оценками типа «высокий», «низкий», «наиболее предпочтительный» и т.д. Тогда параметр описывается как лингвистическая переменная со своим термом-множеством значений [2], а связь количественного значения некоторого фактора с его качественным лингвистическим описанием задается так называемыми функциями принадлежности фактора нечеткому множеству.

Исходя из введенных данных, можно построить полную модель информационной системы компании, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе. Идентифицировав несколько десятков информационных ресурсов, получим в результате анализа сотни или даже тысячи оцененных рисков. Задача осложняется тем, что показателей много, изменяются они зачастую разнонаправлено, и поэтому при анализе стремятся «свернуть» набор всех исследуемых частных показателей в один комплексный, по значению, которого и судить о степени безопасности организации.

2.2 Решение

Для примера рассмотрим задачу определения текущего состояния некоторой организации (предприятия, фирмы ит.п.). Пусть заданы два временных интервала I и II, по которым проводится сопоставительный анализ состояния информационной безопасности организации. Пусть это состояние в каждом из периодов характеризуется набором N показателей, построенных на основании отчетности анализа инцидентов за период. В периоде I это показатели X1, … , XN со значениями xI1, …, xIN , в периоде II - те же показатели со значениями xII1, …, xIIN, причем предполагается, что система показателей {X} достаточна для достоверного анализа (для классификации и сопоставления состояний организации).

Полное множество состояний A организации разбито на пять (в общем случае пересекающихся) нечетких подмножеств вида:

A1 - нечеткое подмножество состояний «предельного неблагополучия»;

A2 - нечеткое подмножество состояний «неблагополучия»;

A3 - нечеткое подмножество состояний «среднего качества»;

A4 - нечеткое подмножество состояний «относительного благополучия»;

A5 - нечеткое подмножество состояний «предельного благополучия».

То есть терм-множество лингвистической переменной «Состояние организации» состоит из пяти компонентов. Каждому из подмножеств A1… A5 соответствуют свои функции принадлежности μ1(V) … μ5(V), где V - комплексный показатель состояния информационной безопасности организации, причем чем выше V, тем «благополучнее» состояние организации. Качественный вид функций μi(V) представлен на рис. 1.

Поставим в однозначное соответствие функции принадлежности μ(V) нечеткое число

$$\beta\left(a_a, a_2, a_3, a_4\right) \tag{1}$$

где a1 и a4- абсциссы нижнего основания, а a2 и a3 - абсциссы верхнего основания трапеции (рис. 1), задающей μ в области с ненулевой принадлежностью носителя V соответствующему нечеткому подмножеству. Вернемся к комплексному показателю V. Ясно, что он функционально или алгоритмически связан с набором исходных X показателей:

$$\begin{aligned} V_I &= \Psi(X_{I1},\ldots,X_{IN}), \\ V_{II} &= \Psi(X_{II1},\ldots,X_{IIN}), \end{aligned} \tag{2}$$

но вид Ψ неизвестен и подлежит установлению.

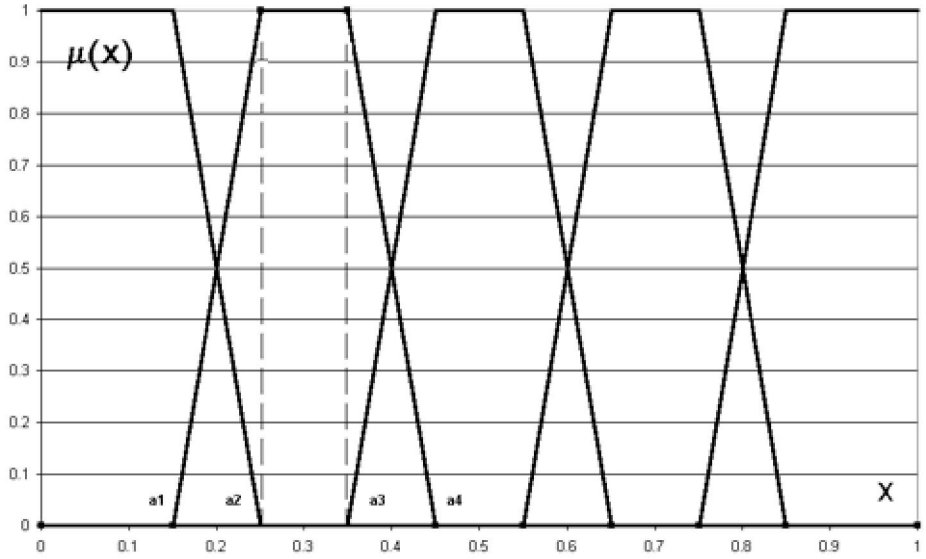

Рисунок 1. Качественный вид функции принадлежности.

В отношении каждого показателя известно, как его изменение влияет на изменение V. В качестве оценки риска ущерба в результате нарушения информационной безопасности введем лингвистическую переменную «Степень риска» со значениями {Наивысшая, Высокая, Средняя, Низкая, Незначительная}. Взаимно однозначное соответствие лингвистических переменных «Состояние организации» и «Степень риска» задана таблицей 1.

Таблица 1. Соответствие лингвистических переменных.

Значение переменной «Состояние организации»	**Значение переменной «Степень риска»**
Предельное неблагополучие	Наивысшая
Неблагополучие	Высокая
Среднее качество	Средняя
Относительное благополучие	Низкая
Предельное благополучие	Незначительная

Тогда задача комплексного анализа состояния информационной безопасности может быть сформулирована следующим образом:

Определить процедуру Ψ (функцию или алгоритм), связывающую набор показателей {X} с комплексным показателем V. Тогда, по мере получения количественных значений V и на основании функций {μ} конструируется следующее утверждение:

«Текущее состояние организации:

предельно благополучно с уровнем соответствия μ1(V),

относительно благополучно с уровнем соответствия μ2(V),

среднего качества с уровнем соответствия μ3(V),

неблагополучно с уровнем соответствия μ4(V),

предельно неблагополучно с уровнем соответствия μ5 (V)».

Это утверждение придает определенный вес каждой из гипотез принадлежности текущего состояния организации к одному из нечетких подмножеств {A}. Лицо, принимающее решение в отношении организации, может удовлетвориться той гипотезой, для которой значение μ(V) максимально, и таким образом для себя качественно оценить состояние организации.

Пусть D(Xi) - область определения параметра Xi, несчетное множество точек оси действительных чисел. Определим лингвистическую переменную «Уровень показателя Xi» с введением пяти нечетких подмножеств множества D(Xi):

B1 - нечеткое подмножество «очень низкий уровень показателя Xi»,

B2 - нечеткое подмножество «низкий уровень показателя Xi»,

B3 - нечеткое подмножество «средний уровень показателя Xi»,
B4 - нечеткое подмножество «высокий уровень показателя Xi»,
B5 - нечеткое подмножество «очень высокий уровень показателя Xi».

Задача описания подмножеств {B} - это задача формирования соответствующих функций принадлежности μ 1-5(xi). В работе использован метод построения функций принадлежности, основанный на статистической обработке мнений группы экспертов [3]. Далее выстраиваются показатели Xi по порядку убывания значимости для анализа и определяются абсциссы трапециевидных Т-чисел (см. рис.1). Принадлежность Т-числа V одному из нечетких подмножеств {A} состояний фирмы определяется с использованием формул пересечения и объединения нечетких подмножеств. В работе использован пакет прикладных программ Fuzzy Logic Toolbox, позволяющий создавать системы нечеткого логического вывода и нечеткой классификации в рамках среды MatLab, с возможностью их интегрирования в Simulink.

3 Заключение

Нечетко-множественный подход к решению многих задач явился ответом на непреодолимые трудности, связанные с использованием вероятностей при учете исходной информационной неопределенности. В данной работе предложен подход к анализу риска ИБ, заместив вероятностный анализ риска на анализ с применением нечетких множеств. Всегда остается возможность поставить под сомнение неограниченную познавательную активность эксперта или лица, принимающего решения. В этом смысле оказалось полезнее не давать вероятностям точечные оценки, а вырабатывать нечетко-лингвистическое описание этих вероятностей, - то есть моделировать не только сам объект исследования, но и границы познавательной активности

Предложенная методика, на самом-то деле, воспроизводит мыслительные человеческие процессы, основанные на субъективных суждениях. Предложенная модель была адекватна не только реалиям объекта исследования, но и специфическим особенностям познающего субъекта, а также формально очерченным границам наличной информационной неопределенности. То, что мы знаем об объекте исследования, и то, как мы это знаем, - все это находит отражение в логико-математических формализмах, на которых основан метод. Распознавание и классификация состояний предприятий - задача, которая вне идеологии нечетких множеств вообще не может быть решена удовлетворительно, потому что прежде чем говорить “плохое” или “хорошее”, необходимо принять соглашение, как различать эти субъективные высказывания.

Литература

[1] Zadeh L.: Fuzzy sets. *Information and Control*. № 8: 338-353, 1965.

[2] Орловский С.А.: Проблемы принятия решений при нечеткой исходной информации. Москва, Радио и связь, 1981. 286 с.

[3] Штовба С.Д.: Проектирование нечетких систем средствами MATLAB. Москва, Горячая линия – Телеком, 2007. 288 с.