

## ЦЕЛЕСООБРАЗНОСТЬ И ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ НЕЧЕТКОГО МОДЕЛИРОВАНИЯ ДЛЯ ОЦЕНКИ РИСКОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

**Владимир Чернов,**

*Владимирский государственный университет  
(Российская Федерация)*

**Александр Дорохов,**

*Харьковский национальный экономический университет  
(Украина)*

*The problem of the analysis, modelling, forecasting of risks in information systems has been examined. Necessity and an opportunity of application of the fuzzy sets theory for studying risks of development, introduction and operation of information systems has been proved. Application of specialized software, such as Matlab Fuzzy Toolbox, Fuzzytech and Fuzicalc, for studying and modelling of corresponding risks in information systems has been offered.*

Изучение разнообразных процессов, этапов и составляющих разработки, внедрения, эксплуатации информационных систем, включая финансово-экономические составляющие, техническую, информационную, экономическую безопасность, надежность и устойчивость работы, сохранения и обработки информации, корректности и адекватности продуцируемых управленческих решений, требует использования новых, научно обоснованных, математически formalизованных подходов и методов.

Одним из современных средств изучения информационных системных являются методы и приемы анализа рисков, позволяющие достичь

максимальной эффективности использования информационных систем в условиях рыночной экономики, поскольку под действием законов рынка в условиях конкуренции результаты внедрения и эксплуатации этих систем в значительной степени связаны с различными рисками и неопределенностью, которые следует учитывать, измерять и оценивать влияние.

Анализ и программирование рисков особенно необходимы для ИТ-компаний, специфика деятельности многих из которых заключается в наличии нескольких рыночных элементов, сегментов (заказчиков, покупателей, потребителей, пользователей) со слабоопределенными

колебаниями объема и структуры спроса в условиях недостатка маркетинговой информации, высокой степени риска при проведении коммерческих операций.

С другой стороны, информационное обеспечение при оценке и программировании риска служит не только в качестве источника данных для анализа, но и само по себе является средством снижения риска. Однако доступ к информации, на основе которой принимаются решения, связанные с выявлением и оценкой текущих и перспективных тенденций в условиях рынка, ограничен, так как получение данных о работе других ИТ-компаний часто затруднено существованием коммерческой тайны, способностью каждой компании в любой момент принять любое решение, непредсказуемое для оценивающего окружающую среду субъекта, что порождает неопределенность при выборе линии поведения и прогнозирования риска.

С позиций системного анализа это означает, что существует многообразие реально существующих и взаимодействующих друг с другом систем, есть вероятность неблагоприятных внешних воздействий, и, следовательно, внешняя среда постоянно создает риски наступления неблагоприятных событий. Совокупность этих систем образует многомерное пространство их взаимодействия в котором находится все многообразие существующих

рисков - многомерное пространство рисков. В нем каждому виду деятельности, касающейся информационных технологий, соответствует свое подпространство рисков.

Подпространства рисков, касающихся информационных технологий, формируются в зависимости от вида или типа информационной системы, стадии ее жизненного цикла (проектирование, разработка, внедрение, эксплуатация, модернизация, ликвидация и так далее), финансовых, социальных, общественных условий и ограничений, отрасли использования, региона, стратегии поведения действующих лиц и принимаемых ими решений. На каждый из рисков оказывает (или может оказывать) влияние своя система факторов. Таким образом, оценивание и программирование рисков для информационных систем - это многофакторная задача, специфика которой заключается в том, что действующие факторы сами по себе могут и не провоцировать развитие рисков ситуации, но при некоторых сочетаниях, которые не всегда можно предвидеть, могут привести к крайне негативным.

Очевидно, что подпространство рисков, в котором происходит любой рассматриваемый вид деятельности, нуждается в создании систем классификации рисков и влияющих на них факторов. Существуют варианты такой классификации и для информационных систем.

Не останавливаясь подробно на этих вариантах, отметим одно существенное обстоятельство. При создании такой классификации фактически происходит замена сложной системы рисков, реально существующих в рассматриваемом подпространстве (т.е. объективной системы), на субъективное и всегда упрощенное отражение этой системы рисков некоторой моделью с целью их практического изучения и анализа.

Использование значительной доли субъективных оценок приводит к тому, что результат анализа риска, связанного с информационными системами, в большой степени имеет характер субъективного исследования, получаемого с различной степенью достоверности, у которой значение не меньше, чем сама полученная результирующая величина (оценка) риска.

На практике приходится иметь дело с конкретной системой рисков конкретной информационной системы. Явно выраженный динамический характер этой ситуации приводит к тому, что во временном смысле области оценка рисков для любой информационной системы связана с задачей прогнозирования, что также предопределяет неопределенность в полученных результатах.

Общий жизненный цикл любой информационной системы от формирования бизнес-идеи до завершения эксплуатационной фазы сопровождается появлением и развитием

различных рисков, поэтому вполне правомерно говорить о существовании целостной и весьма сложной пространственно-временной системы рисков, в рамках которой происходит разработка, внедрение, эксплуатация информационной системы. При этом отдельные риски или их подмножества, объединенные взаимозависимостями, подчиняются своим внутренним, объективным законам, абсолютное познание которых чрезвычайно затруднено.

Все изложенное выше позволяет с полным основанием увязать понятие «риска» в информационных системах с понятием «неопределенность». При этом следует отметить, что очень часто в исследованиях, посвященных различным рискам, понятие «неопределенность» заменяется (не всегда достаточно обоснованно) более узким - «случайность». Ведь только при таком упрощении возможно использовать для оценки рисков в информационных системах методы классической теории вероятностей. Однако остаются до конца не решенными проблемы корректного применения этих методов.

В то же время можно говорить о существенных преимуществах применения теории нечетких множеств (разработки соответствующих многокритериальных моделей и их реализации в специализированных программных продуктах) для оценки рисков в информационных системах.

Основное преимущество такого подхода определяется тем, что аппарат теории нечетких множеств требует от лица, принимающего решения, задания не точечных вероятностных оценок, а интервальных, образующих расчетный коридор значений прогнозируемых параметров. Отсюда вытекает удобство этих методов, проявляющееся в повышенной степени обоснованности, поскольку здесь учитываются все возможные сценарии развития, образующие непрерывный спектр, в отличие, например, от метода Гурвица, рассчитанного на дискретное множество сценариев.

При этом оценки рисков могут быть получены в двух вариантах.

Первый - это величина финансовых, информационных и других потерь, которые возможны в случае нежелательного развития ситуации. Второй - это некоторый числовой или нечисловой показатель, характеризующий уровень риска, присущий анализируемой информационной системе, как степень неопределенности относительно будущего развития позитивных и негативных сторон ее функционирования и окружающей среды. Соответствующие методы оценки и программирования рисков нами в настоящее время развиваются с использованием программного обеспечения Matlab Fuzzy Toolbox, Fuzzytech и Fuzicalc и будут представлены в дальнейших публикациях.

## POLICY OF PERSONAL DATA SECURITY

**Lukasz Kister,**

*European Association for Security (Poland)*

*This article focuses on procedures of drawing up and bringing into effect a document which describes essential rules for personal data security. Possession of such a document is legal obligation to any organization that processes personal data on territory of the Republic of Poland.*

### **1. Introduction**

Once Poland run for joining the European Union structures it had to conform its national legal system to meet the international standards within the area of civil rights and obligations. At level of personal data se-

curity, all EU countries are obliged to implement *Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (WE L 281)*. Poland im-