Таким чином, не існує вразливих значень H, при яких можна однозначно розшифрувати повідомлення без знання особистого ключа.

Зауваження: Біт b^* для формування нового відкритого ключа можна обирати будь-який.

Отже, при застосуванні підходу подвійного шифрування у криптосистемі AJPS вдається уникнути обмежень на значення відкритого ключа, тим самим зменшуючи кількість необхідних перевірок значень параметрів при реалізації криптосистеми.

Література

1. Post-Quantum cryptography standardization NIST [Електронний ресурс]. - 2017. - Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

2. A New Public-Key Cryptosystem via Mersenne Numbers [Електронний ресурс] / D.Aggarwal, A. Joux, A. Prakash, M. Santha. - 2017. - Режим доступу: https://eprint.iacr.org/2017/481.

3. Побудова обмежень на значення відкритого ключа криптосистеми AJPS / Д.В.Ядуха - Теоретичні і прикладні проблеми фізики, математики та інформатики. // Матеріали XVI Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, 26-27 квітня 2018 року, м.Київ, Україна – том 2, ст.81

УДК 004.9:004.75

ЭКСПЕРТНЫЕ ТЕХНОЛОГИИ В МОДЕЛИРОВАНИИ СИСТЕМ

Ю.М. Лисецкий
ДП «ЭС ЭНД ТИ УКРАИНА»

Моделирование является мощным инструментом исследования систем [1]. При моделировании системы, мы осуществляем прогнозирование за счет решения задач идентификации неизвестных зависимостей и их оптимизации на основе статистической и экспертной информации [2]. Моделирование систем является информационно-аналитическим процессом, который базируется на ретроспективных данных, статистической информации о подобных системах, результатах прогнозирования или оценках экспертов, использование которых объясняется, как сложностью исследуемых систем, так и отсутствием надежных экспериментальных данных (рис.1).

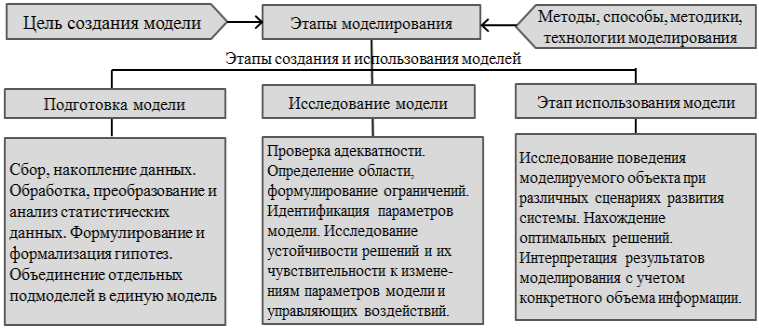

Рисунок 1 – Моделирование систем

В таких случаях экспертные процедуры являются эффективным, а иногда и единственным средством решения задач и требуют привлечения группы высокопрофессиональных специалистов [3]. Основное преимущество групповой оценки заключается в возможности разностороннего анализа как количественных, так и качественных аспектов решаемой проблемы. Но групповая оценка может считаться достаточно надежной только при условии хорошей согласованности мнений участвующих в экспертизе специалистов. Поэтому обработка информации, полученной от экспертов, должна включать в себя оценку степени согласованности мнений и выявление причин их неоднородности [4].

Это можно сделать с помощью статистической обработки информации, полученной от экспертов [5]. В этом случае полученные от экспертов оценки могут рассматриваться как случайная переменная и поэтому для анализа разброса и согласованности оценок применяются следующие статистические характеристики:

– среднее значение оценок (точечная оценка для данной группы экспертов), которое характеризует обобщённое мнение экспертов по альтернативам;

– среднее квадратичное отклонение, характеризующее разброс мнения отдельных экспертов относительно среднего значения;

– коэффициент вариации, характеризующий вариабельность, рассчитываемую в виде отношения среднего квадратичного отклонения оценки к средней арифметической.

С точки зрения математической статистики оценки, существенно отличающиеся от среднего значения могут считаться случайными. Поэтому было введено понятие противоречивости мнения эксперта k

обобщённому мнению всех экспертов, которое основывается на допущении, что мнение y_k эксперта k является крайним среди мнений m экспертов. Анализ противоречивости мнения эксперта k проводится с использованием оценки анормальности результатов при неизвестной генеральной дисперсии.

Для оценки меры сходства мнений экспертов используются коэффициенты ассоциации (по Устюжанинову), с помощью которых учитывается лишь число совпадающих или несовпадающих ответов и не учитывается их последовательность .

Для более точной оценки согласованности мнений экспертов используем методы ранговой корреляции:

1. Коэффициент ранговой корреляции Кендалла, как одну из выборочных мер зависимости двух случайных величин (признаков) X и Y, основанную на ранжировании элементов выборки $(X_1, Y_1),..., (X_n, Y_n)$. Коэффициент ранговой корреляции Кендалла [7] относится к ранговым статистикам и как любая ранговая статистика может использоваться для обнаружения зависимости двух качественных признаков, если только элементы выборки можно упорядочить относительно этих признаков.

2. Коэффициент ранговой корреляции Спирмена, который также является мерой зависимости двух случайных величин, основанной на ранжировании независимых результатов наблюдений, с помощью которого коэффициент вычисляется проще и быстрее.

При анализе оценок, полученных от экспертов, часто возникает необходимость выявить согласованность их мнений по нескольким альтернативам, оказывающим влияние на один конечный результат. В этом случае согласованность мнений экспертов оценивается с помощью коэффициента конкордации W– общего коэффициента ранговой корреляции для группы, состоящей из m экспертов.

Для того, чтобы оценить значимость коэффициента конкордации, пользуются критерием χ^2. Найденное значение должно быть больше табличного χ^2, определяемого числом степени её свободы и уровнем доверительной вероятности. Это подтверждает значимость коэффициента конкордации.

Для ускорения определения согласованности и достоверности экспертных оценок предлагается технология анализа экспертных заключе-

ний путем применения последовательности методов выявления неоднородности мнений экспертов. Сущность технологии заключается в следующем.

В первую очередь необходимо оценить согласованность мнений экспертов с помощью коэффициента конкордации. Если коэффициент конкордации значим, то мнения группы экспертов согласованы и дальнейший анализ можно не проводить.

Если мнения экспертов окажутся не согласованными, то для оценки меры сходства мнений каждой пары экспертов надо рассчитать коэффициенты ассоциации по Устюжанинову.

Для более точной проверки согласованности мнений экспертов необходимо использовать метод ранговой корреляции Спирмена, с помощью которого коэффициент вычисляется проще и быстрее, чем коэффициент ранговой корреляции Кендалла.

При наличии несогласованности мнений экспертов продолжить анализ для выявления причин их неоднородности и провести проверку на противоречивость мнений, в ходе которой выявляются эксперты, мнения которых существенно отличаются от обобщенного мнения группы.

Предложенная технология анализа экспертных заключений путем применения последовательности методов выявления неоднородности мнений экспертов может быть алгоритмизирована, и алгоритм содержит такие шаги:

Шаг 1. Расчет коэффициента конкордации.

Шаг 2. Оценка значимости коэффициента конкордации.

Шаг 3. Расчет коэффициентов ассоциации.

Шаг 4. Оценка мер сходства мнений пар экспертов.

Шаг 5. Расчет коэффициентов ранговой корреляции.

Шаг 6. Оценка согласованности мнений экспертов.

Шаг 7. Расчет обобщенного мнения группы экспертов.

Шаг 8. Проверка мнения эксперта на противоречивость обобщенному мнению группы.

Данный алгоритм был программно реализован на языке C++ [6]. С помощью программной реализации проводились практические исследования, которые экспериментально подтвердили эффективность предложенной технологии.

Таким образом, недостаточные полнота и достоверность информации часто не позволяют применить математические методы для решения задач моделирования. В этих условиях применение экспертных технологий для построения моделей позволяет существенно повысить их адекватность, исследуемым системам. Очевидно, что ответственным этапом в этих случаях, является анализ мнений экспертов, который

включает проверку их согласованности и достоверности. Несмотря на то, что это достаточно трудоемкий процесс, его качественное проведение возможно, с помощью предложенной технологии анализа экспертных заключений, которая позволяет ускорить определение их согласованности и достоверности.

Литература

1.Томашевский В. М. Моделирование систем / Томашевский В. М. − К.: “Вид.гр.БХВ “, 2005. − 352 с.

2. Лисецкий Ю. М. Некоторые подходы к построению моделей сложных систем / Ю. М. Лисецкий // Восьма міждунар. наук.-практ. конф. «Математичне та імітаційне моделювання систем. МОДС’2013», (Київ – Жукин, 24–28 червня 2013 р.). – Київ – Жукин, 2013. – С. 326–330.

3. Китаев Н. Н. Групповые экспертные оценки / Китаев Н. Н. – М.: Экономика, 1975. – С. 64.

4. Литвак Б. Г. Экспертная информация: Методы получения и анализа / Литвак Б. Г. – М.: Радио и связь, 1984. – С. 118.

5. Бешелев С. Д. Математико-статистические методы экспертных оценок / С. Д. Бешелев, Ф. Г. Гурвич. – М.: Статистика, 1980. – 263 с.

6. Лисецкий Ю. М. Об автоматизации экспертных оценок / Ю. М. Лисецкий, Н. П. Каревина // Математичні машини і системи. – 2008. – № 1. – С. 151–162.

УДК 004.773.2

ІНТЕЛЕКТУАЛЬНИЙ МОНІТОРИНГ ДРУКОВАНИХ ТЕКСТІВ

М.С. Голуб

Черкаський державний технологічний університет

Потреба автоматизації процесу обробки інформації, яку містять друковані тексти, роблять актуальними дослідження в області їх інтелектуального моніторингу. Більшість із завдань моніторингу в цій предметній області можна формалізувати як задачі класифікації тексту, крім цього актуальними є задачі структурної та параметричної ідентифікація , прогнозування та інші. Таким чином реалізовуються завдання із пошуку текстів заданої тематики чи заданого змісту, заданого автора, чи групи авторів.

Результати інформаційного пошуку методів та засобів розв’язання завдань інтелектуального моніторингу друкованих текстів дозволяє зробити висновки, що найбільш перспективною технологією інтелектуального аналізу тексту (Text mining) є машинне навчання нейромереж,