

можна розкрити тільки прямим перебором. Крипостійкість в цьому випадку визначається розміром ключа.

Одним з головних переваг цього методу являється те, що час на зашифровування практично дорівнює (а то і дорівнює) часу на розшифровування.

При всіх перевагах - простота реалізації, теоретично гарантована стійкість, зручність застосування цей шифр володіє двома недоліками:

1. Найбільш істотний полягає в тому, що обсяг ключового матеріалу збігається або навіть перевищує обсяг переданих повідомлень. Гамму і зашифрований текст краще передавати по різних захищених каналах. Що значно збільшує вартість.

2. Необхідно мати ефективні процедури для вироблення випадкових рівноймовірно двійкових послідовностей та спеціальну службу для розвезення величезної кількості ключів.

Література

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. *Захист інформації в комп'ютерних системах і мережах*. Під ред. В.Ф. Шаньгіна. - 2-і изд., перераб. і доп. - М.:Радіо і зв'язок, 2001. - 376 с.: іл.

УДК 004.8.032.26; 504.064.36

*А.Л. Ляхов, д.т.н, проф.,
С.П. Алёшин, к.т.н., доцент,
О.О. Бородина, аспірантка,
Т.Е. Александрова, О.В. Лисовой,
студенты гр. 301-ТН
Полтавский национальный технический
университет имени Юрия Кондратюка*

КОНСТРУКТИВНИЙ КРИТЕРІЙ ПРОДУКТИВНОСТІ ІНТЕЛЕКТУАЛЬНИХ СППР

Применение технологий искусственного интеллекта (ТИИ) в управлении сложными социотехническими объектами раскрывает ряд нерешенных теоретических и практических проблем. Основные среди них: нет аналитической взаимосвязи размерности входного вектора, мощности обучающей выборки с числом элементов в скрытых слоях нейросети, значениями ошибок обучения и обобщения, временем итерационного процесса, формы поверхности ошибки отклика сети; отсутствует строгое теоретическое обоснование сходимости процесса обучения сети за конкретное число циклов; при многомерном входном векторе требуется значительное число нейронов в скрытом слое для адекватного отображения искомой функциональной зависимости «вход – выход» по массиву примеров из обучающей выборки, что усложняет форму поверхности ошибки. Проектирование систем поддержки решений в управления сложными объектами осуществляется в условиях отсутствия единых подходов, цельной методологии подготовки данных, выбора архитектуры сети, универсальных аналитических моделей, быстрых и надежных алгоритмов обучения, конструктивных критериев продуктивности.

Так как получить точную математическую модель поведения объекта не всегда представляется возможным применяют аналитический

подход, основанный на прецедентах, содержащих информацию о закономерностях факторов и состояний, их взаимном влиянии, силе и направлении воздействия. Для извлечения этой информации и практического использования в аналитических системах поддержки принятия решений возникает необходимость моделирования базовых функций, являющихся фрагментами искусственного интеллекта:

- описание и представление образа конкретного объекта в форме массива информативных признаков;
- представление образа объекта в форме принадлежности к некоторым смысловым отображениям (классам);
- формирование обобщенных образов объектов на основе использования процедур восприятия и идентификации при описании конкретных объектов на основе примеров (массив выборки пар «вход – выход»);
- оценка дифференцирующей силы признаков и их редукция: определение для каждого признака его вклада в различие друг от друга обобщенных образов; понижение размерности пространства признаков через контролируемое и корректное удаление незначимых признаков;
- классификация обобщенных образов: определение сходств и различий обобщенных образов друг с другом; объединение сходных образов в кластеры (множества со сходными признаками);
- классификация признаков: определение сходств и различий признаков по их смыслу; объединение сходных по смыслу признаков в кластеры;
- распознавание объектов: сравнение предметного образа конкретного объекта со всеми обобщенными образами и принятие решения о принадлежности к классу – выбор оптимальных управляющих факторов: формирование массива возможных управляющих воздействий, анализ их силы и направления, адаптация к предметной области, обеспечение заданных целевых состояний объекта.

Продуктивная реализация отмеченных функций в системах поддержки решений управления ССТС входит в противоречие с их недостаточным методологическим, алгоритмическим и программным обеспечением. Требуют дополнительной теоретической проработки вопросы:

- структуризация и формализация предметной области;
- синтез аналитической модели ССТС;
- выбор состоятельных критериев и оптимизация модели;
- обеспечение и контроль адекватности модели, надежности и точности результатов;
- решение задач идентификации состояния объекта управления, прогнозирование динамики поведения и поддержка принятия управленческих решений с применением обученных моделей;
- нахождение аналитических оценок надежности и точности разрабатываемых процедур анализа данных в сложных социотехнических системах для установления границ применимости разработанных методов, алгоритмов и моделей.

Следовательно, существует проблема создания продуктивных СППР в управлении ССТС, острота которой может быть уменьшена разработкой методов, технологий и программного обеспечения построения моделей, позволяющих автоматизировать базовые процессы при распознавании состояний, прогнозировании динамики поведения и выборе оптимальных

управляющих факторов исследуемых объектов на базе интеллектуальных технологий. При этом необходимо получить оценку продуктивности СППР в управлении ССТС путем интеллектуализации её базовых функций.

Целесообразность интеллектуализации поддержки принятия решений базируется на современных возможностях субъектов принятия решений в контексте большей продуктивности автоматического ПР в сравнении с диалоговым. Как показано в [1] продуктивность автоматического режима в системах компьютерной алгебры с повышением сложности задачи растет за счет повышения интеллектуализации. СППР для управления сложными объектами, как показано в [2,3,4], успешно реализуются на базе искусственных нейронных сетей (ИНС), которые реализуются либо специализированными нейрокомпьютерами либо специальным программным обеспечением обычных компьютеров. Анализируется гипотеза и обосновываются выводы о продуктивном процессе интеллектуализации предварительного анализа входных данных на основе предлагаемых технологий извлечения новых знаний из массивов данных в процессе обучения и самообучения нейросетевых моделей. Приводятся примеры реализации в экологии, технической диагностике, экономике и ансамбль обученных и верифицированных нейросетевых моделей.

Литература

1. В.П.Клименко, О.Л.Ляхов *Интелектуалізація розв'язання складних прикладних задач методами комп'ютерної алгебри.*- Логос, 2009. -293с.
2. А.А. Морозов, В.П. Клименко, А.Л. Ляхов, С.П. Алёшин *Состояние и перспективы нейросетевого моделирования СППР в сложных социотехнических системах.* - *Математичні машини і системи.* – 2010. – № 1. – С. 127 –149.
3. Ляхов А.Л., Алёшин С.П. *Интеллектуальный анализ данных в прикладных экономических задачах / Науковий вісник ПолтНТУ. Економіка і регіон – 2009. - № 4(23). – С. 140 – 147.*
4. Ляхов А.Л., Алёшин С.П. *Сложная социотехническая система как объект управления искусственной нейронной сетью / Вісник інженерної академії України.* – 2010. – № 1. – С. 93 – 97.

УДК 681.513

*Демиденко М.И., старший викладач,
Полтавський національний технічний
університет імені Юрія Кондратюка*

IEDF0 МОДЕЛЬ ПРОЦЕССА СБОРА ДАННЫХ О ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ УЧЕБНЫМ ПРОЦЕССОМ В ВУЗЕ

Существующие информационные системы управления учебным процессом в ВУЗе в полной мере не удовлетворяют предъявляемым к таким системам требованиям. Зачастую эти системы не позволяют учесть специфику организации учебного процесса в конкретном ВУЗе, не обеспечивают интеграцию с системами, функционирующими на государственном уровне. Анализ показывает, что задача управления информационными потоками в ВУЗах по-прежнему остается актуальной проблемой как на уровне системообразующих связей высшей школы, так и на уровне ВУЗа[1].