5. Построение модели связывающей факторы, оказывающие воздействие и результативные факторы

6. Оценку эффективности модели.

7. Повторение пп 1-6.

8. Получение завершающей количественной и качественной оценки влияния факторов, оказывающие воздействие на результативные факторы и принятие решений на этой основе.

Список литературы

1. Thomas F. Ruddy, Lorenz M. Hilty: Impact assessment and policy learning in the European Commission. In: Environmental Impact Assessment Review, Vol. 28, No. 2-3. (2007), pp. 90-105. doi : 10.1016/j.eiar.2007.05.001_5.

2. Поляков А.А., Цветков В.Я. Информационные технологии в управлении. – М.: МГУ факультет государственного управления, 2007 – 138 с.

ОППОЗИЦИОННОЕ И СИТУАЦИОННОЕ ТЕСТИРОВАНИЕ

Цветков В.Я.

ОАО Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (ОАО «НИИАС»), Москва, e-mail: cvj2@mail.ru

Среди множества вариантов тестирования в сфере образования можно выделить две качественные группы: оппозиционное и ситуационное тестирование. Оппозиционное тестирование основано на понятии оппозиционных переменных [1, 2]. Такие тесты основаны на схеме «да –нет». Эта группа тестов требует информационного соответствия [3] между заранее заданным ответом и ответом обучаемого. Эти тесты направлены на проверку знаний нормативов, определений, формул, статей уголовного или гражданского кодекса пр., то есть на развитие памяти и запоминание учебного материала. Как правило, в этих тестах исключена множественность ответов и есть только один правильный ответ. Условие задачи (теста) в них однозначно. Главным в оппозиционном тестировании является проверка запомненных знаний.

Ситуационное тестирование применяет для тестирования модели ситуаций с множеством условий. Эти условия не всегда четкие и семантически информативны [4]. Поэтому, субъект, проходящий тестирование должен их дополнять ситуацию для получения четких условий решения поставленной задачи. Это также является частью тестирования – умение формулировать условие задачи. Ситуационное тестирование допускает множество вариантов ответов и множество путей логического доказательства. Главным в ситуационном тестировании проверка умений строить логику вывода или логическую цепочку вывода. Ситуационное тестирование часто применяют при изучении задач второго рода [5, 6]. В этом случае обучаемый показывает умение эвристических методов решения задач.

Оппозиционное и ситуационное тестирование дополняют друг друга. На этапе получения знаний применяют оппозиционное тестирование. На этапе закрепления и применения знаний применяют ситуационное тестирование. Совместное применение этих групп тестов дает больший эффект, чем применение только оппозиционных тестов.

Список литературы

1. Цветков В.Я. Использование оппозиционных переменных для анализа качества образовательных услуг // Современные наукоёмкие технологии. – 2008. – № 1 – С. 62-64.

2. Tsvetkov V. Ya. Opposition Variables as a Tool of Qualitative Analysis // World Applied Sciences Journal. – 2014. – 30 (11). – p. 1703-1706.

3. Цветков В.Я. Информационное соответствие // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 1 (часть 3) – С. 454-455.

4. Номоконов И.Б., Цветков В.Я. Многоаспектность информативности. // Дистанционное и виртуальное обучение– 2015. – № 12. – С. 74-80.

5. Цветков В.Я. Решение задач второго рода с использованием информационного подхода // Международный журнал прикладных и фундаментальных исследований. – 2014. – №11. (часть2) – С. 191-195.

6. Tsvetkov V.Ya. Incremental Solution of the Second Kind Problem on the Example of Living System, Biosciences biotechnology research Asia, November 2014. Vol. 11(Spl. Edn.), p. 177-180. doi: http://dx.doi.org/10.13005/bbra/1458.

СЕМАНТИЧЕСКАЯ СТРАТИФИКАЦИЯ КАК ИНСТРУМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цветков В.Я.

ОАО Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (ОАО «НИИАС»), Москва, e-mail: cvj2@mail.ru

Стратификация информации широко применяется в разных направлениях [1] (социология, археология, геоинформатика), прежде всего, как инструмент преодоления сложности. При использовании стратифицированной информации для восстановления информативности широко применяется процедура оверлея для композиции страт (слоев). При организации информационной безопасности для обеспечения защиты информации от несанкционированного доступа возможна обратная процедура – декомпозиция информационного массива на страты. Задача взломщика – извлечение смыслового содержания. Если такое содержание в информационном массиве отсутствует, то такая информация может считаться криптографически стойкой [2, 3]. Концептуально семантическая стратификация заключается в разбиении информационного массива на части, не содержащие смысла. Технически такая семантическая стратификация включает: 1) нахождение ключевых смысловых точек. Это могут быть: слова, предложения, фразы. 2) Выделение семантического окружения [4], отвечающего за интерпретацию ключевой точки. 3) Размещение каждой ключевой

точки в отдельном слое. 4) Размещение семантических окружений в разные слои. 5) составление топологической схемы связей слоев для восстановления всего текста. С позиций информативности [5] важными являются связи, которые создают целостные свойства информационного фала как семантической системы

По существу такой механизм состоит в разбиении текста на части, не содержащие семантическую информативность. С позиции знания такая процедура означает трансформацию эксплицитного знания в тацитное [6]. Именно в тацитное, а не имплицитное. Следует отметить, что процедура шифрования может дополнять процедуру семантической стратификации, но не является обязательной. По существу семантическая стратификация является шифрованием без традиционных криптологических технологий

Список литературы

1. Цветков В.Я. Стратификация когнитивной модели // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 2 (часть 1) – С. 136-137.

2. Цветков В.Я. Технологии и системы информационной безопасности. – М.: Минпромнауки, ВНТИЦ, 2001. – 88 с.

3. Цветков В.Я. Защита информации в системах обработки данных и управления. – М.: Миннауки и технологий, ВНТИЦ, 2000. – 64 с.

4. Номоконов И.Б., Цветков В.Я. Многоаспектность информативности. // Дистанционное и виртуальное обучение. – 2015. – № 12. – С. 74-80.

5. Tsvetkov V.Ya. Semantic environment of information units // European Researcher, 2014, Vol.(76), № 6-1, p. 1059-1065 DOI: 10.13187/issn.2219-8229.

6. Сигов А.С., Цветков В.Я. Неявное знание: оппозиционный логический анализ и типологизация // Вестник Российской Академии Наук, 2015, том 85, № 9, – с.800–804. DOI: 10.7868/S0869587315080319.

ЦИФРОВОЕ КЛОНИРОВАНИЕ КАК ИНСТРУМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цветков В.Я.

ОАО Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (ОАО «НИИАС»), Москва, e-mail: cvj2@mail.ru

Защита информации является развивающейся информационной технологией [1, 2]. Одним из инструментов защиты информации считают резервное копирование. Резервное копирование представляет собой зеркальное отображение информации на другой носитель, отчего иногда эту технологию называют зеркалированием. Особенностью резервного копирования является наличие информационного соответствия [3] между исходной и скопированной информацией. Недостатком этого подхода является большой объем и открытость копированной информации.

Цифровое клонирование представляет собой технологию копирования с шифрованием, но не всего объема информации, а только ее содержательной части с копированием наиболее важных информационных точек и топологии между этими точками, которая позволяет восстановить исходную информацию. Цифровой клон представляет собой зашифрованную топологическую модель исходного информационного файла, которая содержит три части: вершины графа, как информационные точки файла, структуру топологии между точками и связи, соответствующие данной топологии. Такой подход позволяет хранить исходный клонированный цифровой файл на разных носителях и восстанавливать его только при наличии или сборе всех трех частей. Это обеспечивает большую защищенность, так как требует больших усилий со стороны.

Клонированный цифровой файл можно рассматривать как информационную конструкцию [4] которая обладает свойством разбиения на независимые части и независимого хранения каждой части. Это уменьшает информационный объем и повышает защищенность информационного файла, так как вскрытие одной части цифрового клона не даст возможность восстановить всю информацию в целом. Клонированный цифровой файл можно рассматривать как сложную систему [5]. С позиций информативности [6] важными являются не все связи, а только те, которые создают целостные свойства информационного фала как системы. Эмерджентность свойство системы в целом, которое состоит в несводимости свойств системы к свойствам ее частей. В данном случае только наличие эмерджентности даст возможность восстановить исходный файл.

Список литературы

1. Цветков В.Я. Защита информации в системах обработки данных и управления. – М.: Миннауки и технологий, ВНТИЦ, 2000. – 64 с.

2. Цветков В.Я. Технологии и системы информационной безопасности. – М.: Минпромнауки, ВНТИЦ, 2001. – 88 с.

3. Цветков В.Я. Информационное соответствие // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 1 (часть 3) – С. 454-455.

4. Tsvetkov V.Ya. Information Constructions // European Journal of Technology and Design, 2014, Vol (5), № 3. – p. 147-152.

5. Монахов С.В., Савиных В.П., Цветков В.Я. Методология анализа и проектирования сложных информационных систем. – М.: Просвещение, 2005. – 264 с.

6. Номоконов И.Б., Цветков В.Я. Многоаспектность информативности. // Дистанционное и виртуальное обучение– 2015. – № 12. – С. 74-80.