деловой игры предлагается постоянно использовать мультимедийный комплекс для усиления эффекта наглядности через демонстрацию различных видеоматериалов.

Дополнительным элементом разработанного образовательного модуля является Интернет-форум на тему «Актуальные проблемы инновационного развития сельских регионов Минской области», с помощью которого происходит постоянное целевое информирование слушателей и осуществляется обратная связь при рассмотрении конкретных проблемных вопросов.

Практика показала, что общий объем финансирования работ при освоении подобного проекта не превышает 5 миллионов белорусских рублей с учетом налогообложения. В то же время экономический эффект от снижения хозяйственных затрат и рационального использования бюджетных инвестиций в районных АПК в отдельных случаях может исчисляться большими суммами, ведь в среднем за год в каждом из районов республики осваивается около 150 млрд бел. руб.

Применение программных компьютерных продуктов в ходе деловой игры целесообразно по ряду причин, как психологического, так и экономического характера:
– руководители белорусских агропромышленных предприятий должны морально «дозревать» до уровня технологий 21 века, так как компьютер и его программное сопровождение — неотъемлемый атрибут организационной культуры современного управленца;
– при переходе на компьютерный вариант ситуационного управленческого анализа темпы принятия экономически обоснованных управленческих решений значительно (в 5–6 раз!) возрастают;
– переобученный на применение компьютерных технологий управленец «вырастает в цене» на рынке труда, что немаловажно при привлечении в агрокомплекс республики стратегических инвесторов.

МЕТРИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ РЕАЛИЗАЦИЙ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

А.А. Тиунчик, *к.ф.-м.н.*
Белорусский государственный аграрный технический университет (г. Минск)

Внедрение систем электронных торгов и развитие электронного документооборота в агропромышленном комплексе делает крайне актуальной проблему обеспечения юридических гарантий подлинности электронного документа. Эта проблема решается за счет использования электронной цифровой подписи (ЭЦП) и применения других средств современной криптографии.

В настоящее время в Республике Беларусь действует стандарт СТБ 1176.2-99, регламентирующий порядок выработки и проверки ЭЦП, а также ряд других технических нормативно-правовых актов (ТНПА), определяющих алгоритмы криптографической защиты информации (ГОСТ 28147, СТБ 1176.1-99, РД РБ 07040.1202-2003 и др.). Согласно действующему законодательству любые программные средства (ПС), реализующие стандартизованные алгоритмы криптографической защиты информации (КЗИ), должны проходить сертификационные испытания на предмет соответствия реализованных в них алгоритмов алгоритмам, установленным в соответствующих ТНПА.

Проверка и оценка качества ПС, реализующих алгоритмы КЗИ, имеет первостепенное значение в ряду мер, направленных на обеспечение безопасности информационных ресурсов. При этом оценка качества ПС, реализующих алгоритмы КЗИ, должна основываться не на субъективной оценке эксперта, а на объективных числовых характеристиках, основанных на метриках качества.

При определении показателей качества ПС необходимо учитывать как требования ГОСТ 28195, так и требования базовых международных стандартов, систематизирующих и регламентирующих качество ПС, в частности, ISO/IEC 9126:1-4 (ISO/IEC 25021-25024). Указанные международные стандарты (в Республике Беларусь действует СТБ ИСО/МЭК 9126) устанавливают ряд метрик для объективной оценки ПС, однако метрики для оценки качества реализаций средств КЗИ представлены в них в недостаточном объеме. Кроме того, установленный в ISO/IEC 9126 подход к вычислению значений метрик показателей качества является упрощенным и не позволяет объективно и в полной мере оценить качество ПС.

Вычисление значений метрик показателей качества, применяемое в ISO/IEC 9126, сводится к вычислению отношения числа испытаний, в которых зафиксировано наступление некоторого события, к общему числу проведенных испытаний. Полученное отношение может принимать значение от 0 до 1. По сложившейся практике результаты проверки ПС, реализующего алгоритм КЗИ, считаются положительными, если все показатели качества этого ПС равны единице. Однако такая оценка не является объективной по ряду причин. Во-первых, она не отражает объем и полноту проведения испытаний. Во-вторых, она не учитывает номенклатуру показателей характеристик качества, по отношению к которым проводятся испытания. При разработке метрик показателей качества ПС, реализующих стандартизированные средства КЗИ, необходимо учитывать не только функциональность как наиболее важную характеристику ПС, но и другие характеристики, главным образом связанные с тем, как и при каких условиях заданные функции могут выполняться с требуемым качеством. Необходимо также предусмотреть аналитические средства получения комплексных и интегральных показателей качества, а также наличие шкал оценок, позволяющих производить сравнение ПС КЗИ в целом и по различным параметрам.

Для оценки качества ПС, реализующих алгоритмы КЗИ, необходимо применять комплексные и интегральные показатели качества, отражающие не только функциональность, установленную на минимальном множестве тестов, но и отражающие объем проведенного дополнительного тестирования, разнообразие применяемых при испытаниях тестов, количество специальных проверок на наличие умышленных ошибок, сложность программного кода (включение ассемблерных вставок, многочисленные условные переходы и т.д.) и др.

Задача нахождения ошибок в программных реализациях средств КЗИ является одной из наиболее актуальных и сложных. Среди ошибок, вносимых при создании программных продуктов, встречаются как непреднамеренные ошибки (например, связанные с искажением логики криптографического алгоритма при написании программного кода или неверной организацией ввода и вывода данных), так и умышленные (например, связанные с внесением в программный код недокументированных возможностей или с искажением выполнения криптографического алгоритма в целях повышения быстродействия программной реализации).

Нахождение умышленных ошибок является одной из наиболее трудоемких задач тестирования. Для обнаружения таких ошибок часто применяется непроизводительный и дорогостоящий метод анализа исходных текстов. Однако применение предварительного анализа реализуемого криптографического алгоритма в ряде случаев позволяет предсказать, какие элементы этого алгоритма являются наиболее вероятными с точки зрения возможности внесения в них умышленных ошибок, и разработать тестовые последовательности, позволяющие быстро и достоверно устанавливать факт существования умышленной ошибки.

Процесс разработки тестовых последовательностей для обнаружения умышленных ошибок в программных реализациях криптографических алгоритмов может быть разделен на три этапа:

– нахождение элементов алгоритма, потенциально опасных с точки зрения возможности внесения умышленных ошибок;

– генерация числовых последовательностей *N*, позволяющих однозначно установить факт существования предполагаемой умышленной ошибки в исследуемом участке программного кода;

– генерация исходных параметров алгоритма, обеспечивающих поступление последовательностей *N* в качестве входных данных на требуемый участок программного кода, что позволяет тестировать всю реализацию криптографического алгоритма как «черный ящик».

В качестве примера рассмотрим задачу генерации тестовых последовательностей для нахождения умышленной ошибки в реализации алгоритма СТБ 1176.2.

Алгоритм формирования электронной цифровой подписи согласно СТБ 1176.2 включает в себя следующие основные вычислительные шаги: выработка случайного секретного числа *k;* возведение числа *a* в степень *k* по алгоритму Монтгомери $t := a^{(k)}$; вычисление значения функции хэширования от конкатенации *t* и *M*, где *M* — подписываемое сообщение; вычисление числа

$$V := (k - x \cdot U) \bmod q . \qquad (1)$$

Наиболее сложным вычислительным шагом алгоритма формирования подписи является реализация приведения по модулю *q* числа *N*, где $N = k - x \cdot U$, при выполнении операции (1). Для реализации этой операции часто используется алгоритм, описанный в книге Д. Кнута «Искусство программирования». Этот алгоритм включает обязательную проверку

одного редко выполняемого условия. В целях повышения быстродействия может быть допущено умышленное невыполнение этой проверки. Тестирование на случайно выбранных тестовых последовательностях обеспечивает обнаружение такой умышленной ошибки с вероятностью всего лишь 2^{-15} (при использовании 16-разрядных чисел).

Разработка тестовых последовательностей для обнаружения такой ошибки включает решение двух задач: построение тестовых последовательностей *N*, на которых невыполнение проверки ведет к получению неверного результата операции (1); нахождение таких исходных значений параметров криптографического алгоритма, при подаче которых в качестве исходных параметров алгоритма СТБ 1176.2 на вход операции (1) поступали бы тестовые последовательности *N*.

Построение тестовых последовательностей *N* принципиальных сложностей не вызывает. Рассмотрим решение второй задачи.

При реализации алгоритма СТБ 1176.2 используется значение секретного ключа *x*, секретного числа *k* и числа *M*, на основе которых осуществляется вычисление значения функции хэширования *U*, а затем и значения *N*. Так как требуемое значение *N* определено заранее, то требуется выбрать такие значения чисел *x*, *k* и *M*, чтобы получить нужное значение *U*, что ведет к необходимости решения задачи нахождения коллизии.

Однако анализ алгоритма СТБ 1176.2 показывает, что при фиксации других параметров задача подачи последовательности *N* в качестве входной для операции (1) позволяет не искать коллизию. Последовательность действий должна быть следующей: выбираем *k*, генерируем *t*, выбираем *M*, вычисляем значение функции хэширования *U*. Значение *k* изменить теперь нельзя, так как оно использовано при вычислении *U*. Однако при этом остается возможность выбрать *x* таким образом, чтобы при фиксированных значениях *k* и *U* было получено необходимое значение *N*. Для этого из уравнения $V = (k - x \cdot U) \bmod q$ находим *x*: $x = (k - V)U^{-1} \bmod q$.

Таким образом, применение в ходе испытаний специально разработанных тестовых последовательностей позволяет существенно ускорить и повысить качество тестирования средств КЗИ, а применение расширенного множества метрик и построенных на их основе комплексных и интегральных показателей качества позволяет существенно повысить уровень достоверности оценки качества ПС КЗИ.

Проблема разработки метрик оценки качества ПС для реализации стандартизованных криптографических алгоритмов в ряде случаев выходит за рамки оценки ПС алгоритмов, строго зафиксированных в ТНПА, и требует введения метрик для алгоритмов, реализация которых в ТНПА не приводится. Так, например, в алгоритмах ЭЦП и формирования общего ключа вместо операции умножения применяется операция $\circ$ (операция Монтгомери), определенная для любых элементов $c \in B_p$ и $d \in B_p$ по формуле:

$$c \circ d = (c \cdot d \cdot 2^{-(l+2)}) \bmod p, \qquad (2)$$

где B_p — множество, состоящее из чисел 1, 2, ..., $p - 1$, *l*, *p* — параметры.

Действующие в настоящее время в Республике Беларусь ТНПА не регламентируют способ реализации операции Монтгомери. При этом в настоящее время известно большое количество различных реализаций операции $\circ$. Необходимо отметить, что реализация этой операции в соответствии с формулой (2) является неэффективной. В качестве более эффективной реализации операции $\circ$ можно привести представление операции $c \circ d$ в виде:

$$c \circ d = \frac{cd + cd(-p)^{-1} \bmod m \cdot p}{m} \bmod p.$$

Эффективность реализации операции $\circ$ во многом определяет эффективность реализации всего криптографического алгоритма в целом. Поэтому существует необходимость выбора наиболее эффективного метода реализации этой операции. Для повышения эффективности реализации операции Монтгомери часто применяются крайне сложные методы современной математики, потенциально опасные с точки зрения возможности допущения ошибок при их реализации. Так как действующие в настоящее время в Республике Беларусь ТНПА не регламентируют способ реализации операции Монтгомери, то возникает проблема введения метрик для оценки качества программных реализаций этой операции.

Таким образом, оценку качества ПС, реализующих алгоритмы КЗИ, необходимо проводить на основании метрик показателей качества, обеспечивающих получение объективных

числовых характеристик ПС. В номенклатуру оцениваемых показателей качества могут быть включены следующие: объем и полнота проведения испытаний (выражающие, например, правильность вычислений при проверке на эталонных входных и выходных последовательностях, а также правильность вычислений при нагрузочном тестировании с применением случайно сгенерированных входных данных) наличие в реализации умышленных ошибок, качество реализации алгоритмов, не описанных в ТНПА.

АКТИВИЗАЦИЯ МАРКЕТИНГОВОЙ ДЕЯТЕЛЬНОСТИ НА РЫНКЕ ТРУДА КАК ВАЖНЕЙШИЙ ФАКТОР ЕГО ФОРМИРОВАНИЯ И РЕГУЛИРОВАНИЯ

Л.В. Трейер, *к.э.н., доцент*
Белорусский государственный аграрный технический университет (г. Минск)

Рынок труда — один из наиболее сложных элементов рыночной экономики. Переплетение интересов работника и работодателя при найме и увольнении, циклически изменяющееся состояние экономики, уровень инвестиционной и инновационной активности, динамика трудовых доходов населения, сложившиеся традиции и другие факторы оказывают существенное влияние на структуру и содержание рынка труда.

Принципиальной особенностью рынка труда является то, что его составляющими являются непосредственно живые люди, которые не только выступают носителями рабочей силы, но и наделены специфическими особенностями: психофизиологическими, социальными, культурными, религиозными, политическими и др. Эти особенности оказывают существенное влияние на мотивацию и степень трудовой активности людей и отражаются на состоянии рынка труда в целом.

Наличие и взаимодействие элементов рынка труда необходимо для нормального его функционирования, под которым понимается положение, когда созданы все условия для выполнения функций рынка труда. К ним относятся: организация встречи продавцов и покупателей труда; обеспечение конкурентной среды внутри каждой из сторон рыночного взаимодействия; установление равновесных ставок заработной платы; помощь в решении вопросов занятости населения; осуществление социальной поддержки безработных.

Таким образом, рынок труда, подчиняясь в целом законам спроса и предложения, по многим принципам механизма своего функционирования представляет собой специфический рынок, имеющий ряд существенных отличий от товарных рынков. Здесь регуляторами являются факторы не только макро- и микроэкономические, но и социальные и социально-психологические, не всегда имеющие отношение к цене рабочей силы — заработной плате.

Становление рынка труда в Республике Беларусь — длительный, сложный, противоречивый и многоплановый процесс. Суть его — переход к рынку труда с ограниченным спросом на труд. Этот процесс определяется специфическим характером экономики и структурой народного хозяйства. Он сопровождается рядом объективно сложившихся трудностей структурного, экономического, регионально-миграционного, социально-политического и психологического характера.

Главное противоречие развития рынка труда состоит в специфике переходного периода к рыночной экономике. В этих условиях рынок труда породил новую форму производственных отношений — как между государством и субъектами хозяйствования, так и между предприятиями и трудящимися. Эти вновь возникшие отношения породили массу противоречий, которые охватывают все стороны воспроизводства рабочей силы, ее трудового потенциала.

Республиканский рынок труда характеризует ситуацию с занятостью населения Беларуси в целом. Он является объектом детального рассмотрения и анализа в увязке с другими макроэкономическими процессами, происходящими в стране.

Численность занятых в экономике в январе — мае 2009 г. по сравнению с аналогичным периодом 2008 г. увеличилась на 3,9 тыс. чел и составила 4578,9 тыс. при целевом параметре на 2009 г. 4580–4650 тыс. чел. Вместе с тем, несмотря на прием 20,9 тыс. чел. на дополнительно введенные рабочие места, в движении работников наметилась тенденция превышения численности уволенных над численностью принятых (на 19тыс. чел. в январе-мае 2009 г.)