

ния нагружения, а при высоких частотах это время мало для того, чтобы произошла деформация, так что результирующее повреждение может быть меньше. Этот эффект имеет более важное значение при высоких температурах.

3. Влияние концентрации напряжений

Концентрация напряжений в зерне, связанная с дефектами, как правило, приводит к снижению предела выносливости. Необходимо отметить, что усталостная трещина сама по себе является надрезом, вызывающим высокую концентрацию напряжений. В области концентратора повышается локальное напряжение в материале. Фактическое напряжение у вершины концентратора σ_{\max} значительно больше номинального σ_n коэффициентом концентрации напряжений при их упругом распределении.

4. Влияние контактного трения

В практике часто циклической нагрузке подвергаются зерна, прошедшие через металлические поверхности. В этом случае из-за контактного трения поверхностные слои зерен разрушаются.

Наличие контактного трения при циклическом нагружении в общем случае приводит к снижению циклической прочности зерна.

Таким образом, для оптимального проектирования элементов конструкции зерноочистительных машин и агрегатов, сопряженных с обрабатываемой культурой, следует учитывать поведение обрабатываемого материала при статических и динамических деформациях и при каких-либо более сложных видах нагружении.

ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ ОБУЧАЮЩЕЙ СИСТЕМЫ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кистерова С.Н., Грицык В.А.

В современном информационном обществе, в том числе в образовательной сфере, сложившаяся система обучения специалистов в области информационной безопасности не в состоянии обеспечить необходимый уровень их профессиональной подготовки на основе традиционных видов учебно-методического обеспечения. Данный факт обуславливает необходимость разработки и использования инфокоммуникационных образовательных технологий, обеспечивающих формирование высокой профессиональной компетентности специалистов по защите информации с использованием в образовательном процессе вузов интеллектуальных обучающих систем.

Анализ работ отечественных и зарубежных исследователей позволил сделать вывод о том, что интеллектуальные обучающие системы (ИОС), как новые образовательные технологии способны обеспечить новое качество образования будущим специалистам в области информационной безопасности, к подготовке которых во всем мире сегодня предъявляются повышенные требования. Специфика ИОС заключается в моделировании процесса обучения, при использовании динамически развивающейся базы знаний, а так же автоматический подбор рациональной стратегии и личной индивидуальной траектории обучения, автоматизированный учет и анализ новой информации, поступающей в базу данных. Кроме того, интеллектуальные обучающие системы позволяют решать локальные задачи самостоятельной подготовки студентов и контролировать уровень повышения их профессионального мастерства. Эти системы могут управлять обучением студента, как с точки зрения решения проблемных ситуаций, с которыми им предстоит встречаться в своей будущей профессиональной деятельности, так и осуществлять контроль над самостоятельной работой студентов.

Таким образом, основная задача, которая встает перед современным преподавателем - это оптимальный и обоснованный выбор тех организационных форм обучения и использование таких инновационных технологий и методов в учебном процессе, которые бы обеспечили эффективное усвоение профессионально-значимых знаний, умений, навыков, необходимых будущему специалисту в любой профессиональной деятельности. Использование интеллектуальной обучающей системы как методического руководства самостоятельной подготовки студентов не просто обеспечивает эффективное усвоение профессионально-значимых знаний, умений, навыков, необходимых будущему специалисту в любой профессиональной деятельности, но и превращается роль преподавателя в роль организатора учебной деятельности студента, с действенным инструментом, позволяющим достичь высоких показателей качества обучения.

ПРИМЕНЕНИЯ КОМБИНИРОВАННЫХ МЕТОДОВ ЗАЩИТЫ ПРОГРАММНЫХ ПРОДУКТОВ ОТ НЕЛЕГАЛЬНОГО КОПИРОВАНИЯ

Романенко Д.А., Грицык В.А.

Проблема нелегального использования программных продуктов возникла в 80-х го-

дах XX века, одновременно с появлением персональных ЭВМ, во многом из-за особенностей данного класса компьютеров. Произошло это благодаря стандартизации аппаратного обеспечения и массовому распространению ПЭВМ, поставляющихся без программного обеспечения.

Наиболее эффективным оказывается программно-технический метод. На этапе разработки в программу внедряется фрагмент кода, проверяющий условия её использования, и блокирующий её работу, в случае не соответствия условий лицензии.

В настоящее время существует несколько классов программно-технической защиты. Но каждый из них имеет свои недостатки, например один серийный номер может использоваться на нескольких компьютерах.

Для наиболее эффективной защиты программного продукта целесообразно использовать комбинацию нескольких классов. Одна из самых надёжных комбинаций — объединения криптографической защиты исполняемого кода и внешнего аппаратного устройства, выполняющего функции электронного ключа и внешнего вычислительного модуля, выполняющего часть вычислений, необходимых программному продукту. Данный способ не подвержен типичным атакам на программное обеспечение, таким как дезассемблирование, отладка, анализ дампов памяти, в силу защиты исполняемого кода стойкими криптографическими алгоритмами [2]. А перехват информации, передаваемых между компьютером и ключом не приносит желаемого результата для злоумышленника, так как ключ выполняет вычислительные функции.

АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ ДЛЯ ЛИКВИДАЦИИ АВАРИЙНЫХ РАЗЛИВОВ НЕФТИ

Селуянов А.А.
*Уфимский ГНТУ
Уфа, Россия*

Каждый из объектов транспортировки нефти представляет потенциальную опасность, связанную с возникновением ЧС, обусловленными разливами нефти и нефтепродуктов. Большинство из них находятся в эксплуатации

более 20 лет. Территория транспортировки и перевалки нефти и нефтепродуктов в обозримом будущем не станет экологически безопасной, вследствие сложности и затратности технических и организационных мероприятий. Единственным экономически приемлемым способом борьбы с разливами нефти, в настоящее время, является наличие на потенциально опасных объектах сил и средств, готовых к оперативному перемещению и применению, а также наличие заблаговременно разработанных, эффективных планов ликвидации аварийных разливов нефти (ПЛАРН).

Согласно требований, время локализации разлива нефти на почве не должно превышать 6 часов. За это время должен быть выполнен огромный объем работ. По мнению автора, существующие на предприятиях ПЛАРНы «неповоротливы» в оперативном плане и не могут считаться точными применительно к конкретным участкам трубопровода относительно географических и навигационно-гидрографических свойств местности. В связи с этим вопрос качественного прогнозирования, оперативного предупреждения и своевременной ликвидации аварийных разливов нефти и нефтепродуктов является важным и актуальным.

В этих целях для оперативного решения задач по определению объемов разлитой нефти, количеству сил и средств, моделированию ситуации разлива с учетом географического расположения объекта по отношению к близлежащим населенным пунктам и объектам жизнеобеспечения, геологического строения территории, рельефа, наличия водных объектов и подземных вод как источников водоснабжения, анализу воздействия разливов нефти на различные объекты, наиболее удобным инструментом являются геоинформационные системы (ГИС), которые, используя современные компьютерные технологии, позволяют не только моделировать последствия аварийных ситуаций, но и оценить экологический и экономический ущерб. Результаты моделирования аварийных ситуаций при эксплуатации нефтепроводов являются основой для оценки вредного воздействия аварийных разливов на население и территорию, а также планирования мероприятий по ликвидации последствий этого разлива (локализация и сбор разлившейся нефти, ликвидация нефтешлама, расчет сил и средств для этих работ).