– сформировать и провести оперативное издание расширенных бумажных вестников/журналов/каталогов по результатам проведенных мероприятий и их адресную доставку представителям профессиональной отрасли, включая регуляторов отрасли;

– обеспечить конверсию посетителей off-line семинаров/конференций, на единый on-line ресурс путем размещения уникального контента по результатам проведенных мероприятий;

– обеспечить репутацию единого on-line ресурса путем проведения вебинаров, оперативного представления уникальной профессиональной информации, оперативных ответов на вопросы пользователей со стороны экспертов;

– обеспечить «вирусную» масштабируемость репутации единого on-line ресурса через социальные сети и СМИ, включая ведомственные;

– построить уникальные адресные образовательные off-line программы повышения квалификации в рамках дополнительного образования взрослых с обязательным предварительным анкетированием потребностей и последующей обратной связью от целевых потребителей образовательной услуги;

- проводить оперативный мониторинг, сбор и анализ потребностей профессионального сообщества через форумы/опросы/статистику с передачей итоговых тенденций по качеству услуг, недостатков НПА (ТНПА) регуляторам отрасли для дальнейшего реагирования.

Практическая реализация, верификация и адаптация представленного выше подхода была проведена в 2011-2012 гг. совместно с Департаментом охраны МВД, журналом «Технологии безопасности», БГУИР и другими организациями в рамках научно-практических семинаров: «Комплексная безопасность банков», «Центры обработки данных», «Безопасный город», «Видеоаналитика в системах защиты объектов различных категорий» и научно-практической конференции «Безопасность многофункциональных и спортивных объектов с массовым пребыванием людей».

РОЛЬ ЧЕЛОВЕКА В СИСТЕМЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ АЭС

Э.П. КРЮКОВА

При обеспечении безопасности компьютерных систем АЭС необходимо особо учитывать роль человека в использовании их уязвимостей, возможностей реализации угроз, а также ошибок.

Исследования в области живучести систем управления реакторными установками АЭС уделяют основное внимание разработке программного обеспечения для компьютерных систем, важных для безопасности: обнаружение вторжения, предотвращение вторжения, более строгие системы аутентификации, более стойкие методам шифрования и др., но недостаточно исследований посвящено человеку. Исследования и отчеты идентифицировали человеческую ошибку как причину номер один нарушений правил безопасности. Оценки их влияния, связанного с нарушением правил безопасности, составляют 63–80%.

Как только произошел отказ и началось восстановление компьютерной системы, ошибка человека может сыграть разрушительную роль при восстановлении данных. Отмечается, что 30% всех потерь данных — результат человеческой ошибки и только 15% — от злоумышленного воздействия (вирусное повреждение — 6% плюс кража с использованием компьютера — 9%). Эти ошибки могут быть активными, происходящими в ходе процесса восстановления, или скрытыми, которые следуют из предыдущего процесса архивирования или резервирования.

При анализе угроз следует также учитывать и положительное влияние действий человека при обеспечении защиты компьютерных систем АЭС. Будучи самым слабым звеном компьютерной системы, оператор или служащий может стать преградой, предотвращающей отказ системы или ее компрометацию.

В связи с этим возрастает задача повышения культуры безопасности, которая характеризует квалификационную и психологическую подготовленность работников (персонала), при которой обеспечение безопасности является приоритетной целью и внутренней потребностью каждого, приводящей к осознанию личной ответственности и к самоконтролю в процессе всех работ, влияющих на безопасность.

Система управления безопасностью на предприятии (в организации) должна использоваться для поддержки высокой культуры безопасности, для чего необходимо:

– обеспечить общее понимание ключевых аспектов культуры безопасности в пределах предприятия (организации);

– обеспечить ресурсы для поддержки отдельных членов персонала и групп в выполнении ими задач безопасно и успешно, принимая во внимание взаимодействие между отдельными лицами, технологией и организацией;

– усилить изучение и исследование отношения к проблеме безопасности на всех уровнях организации;

– обеспечить средства для непрерывного развития и повышения культуры своей безопасности.

Знания особенностей персонала и принципов обеспечения надежности человека должны использоваться для повышения качества разработки курсов обучения безопасности и осведомленности и гарантировать восстановление систем с наименьшим ущербом, имущественным и человеческой жизни.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ ПО ОСНОВАМ УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ С УКЛОНОМ В ПРАКТИКУ ЗАЩИТЫ ИНФОРМАЦИИ

Д.Н. МАРУДА, В.Л. НИКОЛАЕНКО, Г.В. СЕЧКО

Подготовка, переподготовка и повышение квалификации кадров в области защиты информации включает изучение курса «Основы управления интеллектуальной собственностью» (ОУИС) в виде отдельной дисциплины или в виде совмещения её с курсом защиты информации «Основы защиты информации и управления интеллектуальной собственностью (ОЗИиУИС)» [1]. При этом, если теоретическая часть курсов ОУИС и ОЗИиУИС представлена в литературе достаточно полно [2, 3], то поиск соответствующего материала для проведения практических занятий (ПЗ), интересного не только для обучающих, но и для обучаемых, — это довольно сложная задача. Поэтому студенты и курсанты большинства учреждений образования республики на ПЗ, посвящённых составлению и оформлению заявок на объекты промышленной собственности (ОПС), выполняют одну и ту же простейшую процедуру: примерно 80 % учебного времени изучают методическое пособие, и затем в течение примерно 10 % учебного времени (в среднем 9 мин) заполняют бланк заявки по установленной форме. Вариантов выполнения задания нет. Виды предлагаемых для включения в заявку ОПС чаще всего не совпадают с тематикой специальности, которую получают обучаемые.

Для устранения данного недостатка в [1, 4] предложено составлять на ПЗ формулу изобретения и реферат ОПС для включения в заявку. Сделанные предшественниками наработки в области составления заявки на ОПС учтены