

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 обучающихся, 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

следующим образом: для составленной студентом однозвенной формулы изобретения ему предлагается заполнить бланк заявки, подписанный заявителем, а затем для предварительно составленной им же многозвенной формулы — бланк, подписанный патентным поверенным. В докладе рассматривается практическая реализация сделанного предложения в виде готового описания ПЗ. в описании предлагается 34 варианта исходных данных для составления сначала однозвенной, затем многозвенной формулы изобретения и реферата на ОПС в области защиты информации и информационной безопасности в телекоммуникациях. Описание прошло практическую апробацию в осеннем семестре 2011 года. Готовятся аналогичные исходные данные для других специальностей и специализаций.

### **Литература**

1. Гасенкова И.В., Лыньков Л.М., Мухуров Н.И., Сечко Г.В. // Закон и порядок: Материалы I Межд. науч.-практ. конф. (31 января 2011 года): Сборник научных трудов. М.: Спутник+, 2011. С. 107-110.
2. Лыньков Л.М., Мухуров Н.И. Лекции по курсу «Основы управления интеллектуальной собственностью» для специальностей 45 01 03 «Сети телекоммуникаций», 98 01 02 «Защита информации в телекоммуникациях». Минск: БГУИР, 2008. 173 с.
3. Герасимова Л.К. Основы управления интеллектуальной собственностью: учеб. пособие. Минск, 2011. 256 с.
4. Корсаков А.В., Маруда Д.Н., Иванова Т.Н. // Тезисы докладов 48-й научной конференции аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии / под ред. В.Л. Николаенко и Г. В. Сечко. Минск: ИИТ БГУИР, 2012. С. 30.

## **ОСОБЕННОСТИ ДИСЦИПЛИНЫ «ФУНКЦИОНАЛЬНЫЕ УСТРОЙСТВА И ЭЛЕКТРОПИТАНИЕ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ» ДЛЯ СПЕЦИАЛЬНОСТИ «ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ»**

Н.И. ШАТИЛО

Современные тенденции развития систем электропитания характеризуются, во-первых, возрастающим использованием цифровых способов контроля и управления, и во-вторых, широким внедрением устройств защиты от помех в связи с усложняющейся помеховой ситуацией в сетях электропитания общего пользования.

Естественные импульсные помехи, наводимые в электрических сетях от молний, и помехи искусственного происхождения, возникающие от воздействия мощных электромагнитных импульсов, например, при коротком замыкании высоковольтной линии электропередачи, соизмеримы друг с другом и достигают единиц килоджоулей.

Эти помехи в первую очередь воздействуют на блоки питания телекоммуникационной аппаратуры, причем это воздействие может быть катастрофическим — энергия разрушения современных интегральных микросхем составляет единицы — сотни микроджоулей.

Поэтому во второй части программы дисциплины предусмотрен специальный раздел, посвященный защите блоков питания от непреднамеренных помех. В этом разделе рассматриваются параметры стандартизованных видов помех: импульсных (микросекундных, наносекундных) и длительных (перепадов сетевого напряжения), помехоустойчивые структурные и схемотехнические решения блоков питания.

Цифровые элементы устройств электропитания особенно чувствительны к внешним импульсным помехам и, в свою очередь, являются источниками таких помех. Поэтому в дисциплине анализируются схемотехнические и конструктивные решения цифровых блоков, обеспечивающие повышенную помехоустойчивость этих блоков и минимальный уровень собственных помех.