Предисловие

В проблематике обеспечения информационной безопасности телекоммуникационных систем на первый план выходят задачи информационной безопасности систем и сетей с радиодоступом. Связано это с несколькими причинами. Прежде всего с широким и все расширяющимся спектром таких систем и сетей, используемых в экономике страны. Это системы и сети сотовые и транкинговые, сети, использующие комплексы спутниковых ретрансляторов, а также сети Wi-Fi, Wimax и т. п. Вторая причина связана с естественной уязвимостью таких систем и сетей — открытым радиоканалом, очень привлекательным для злоумышленников. Эта уязвимость порождает генерацию широкого спектра атак, основанных на формировании и использовании имитационных сигналов.

Далее, современные технологии и развитие жесткой конкурентной среды как между государствами, так и между предприятиями, вызвавшей, по существу, постоянные информационные войны, привело к быстрой сменяемости видов и форм атак, требуют создания телекоммуникационных систем нового поколения. Такие телекоммуникационные системы должны:

во-первых, интегрировать необходимые свойства обеспечения информационного взаимодействия со свойствами необходимого уровня защищенности этого взаимодействия, а

во-вторых, обладать свойством адаптации к изменяющимся видам и формам вредоносного воздействия злоумышленников на основе их обнаружения и исследования в реальном времени.

Естественно, такой подход требует генерации и привлечения новых идей и принципов построения телекоммуникационных систем и технологий их реализации. При этом указанные процессы должны быть высокоскоростными, в противном случае неизбежен проигрыш сопернику.

Существующие традиционные подходы, базирующиеся на макетировании и исследовании макетов новых идей для их доведения до практического использования приведут к неизбежному поражению в информационной войне. В этом случае представляется продуктивной технология проектирования компонентов телекоммуникационных систем и сетей с радиодоступом, базирующаяся на использовании устройств и систем, реализующих принципы программно управляемого функционала и соответствующего программного обеспечения, позволяющего реализовать необходимую управляемость.

Сущность технологии прототипирования заключается в создании макета проектируемой системы, полностью выполняющей все функции на физическом уровне, используя программно-управляемые устройства. Это позволяет с помощью относительно небольшого комплекта устройств и программ, управляющих ими, сформировать инструментарий для проектирования с макетированием и исследованием широкого спектра устройств и систем с существенным сокращением временных затрат. При этом стоимость такого процесса несоизмеримо ниже стоимости изготовления аппаратных макетов.

Такое проектирование практически на физическом уровне крайне важно для систем с радиодоступом, с множеством точек доступа и высокой вероятностью вторжений, требующего сложного поиска решений с большим объемом исследований.

В предлагаемом вашему вниманию учебном пособии представлено построение и технология использования учебно-исследовательского стенда для изучения технологии устройств и систем, построенного на основе одного из вариантов, наиболее современного, по нашему мнению, на сегодняшний момент, сочетающего комплект программируемых устройств с соответствующими средствами программного управления.

Учебное пособие рекомендовано Федеральным учебно-методическим объединением в системе высшего образования по УГСН 10.00.00 «Информационная безопасность» для реализации основной профессиональной образовательной программы высшего образования по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» и направлению подготовки 10.03.01 «Информационная безопасность»,

профиль «Безопасность телекоммуникационных систем». Пособие будет также полезно использовать для реализации следующих образовательных программ и направлений: бакалавриата 11.03.02 «Инфокоммуникационные технологии и системы связи», профиль «Программно-защищённые инфокоммуникации», и магистратуры 11.04.02 «Инфокоммуникационные технологии и системы связи», профиль «Кибербезопасность инфокоммуникаций».