И. А. Кожевников

НЕКОТОРЫЕ АСПЕКТЫ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ТЕХНИЧЕСКИХ СРЕДСТВ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В современных условиях постоянного возрастания угроз осуществления в отношении важных государственных объектов различных противоправных действий (хищения и порча уникального оборудования, съем конфиденциальной информации, диверсии, террористические акты и прочее) весьма актуальной является задача надежного противодействия указанным угрозам посредством эффективного применения систем физической защиты (СФЗ).

Современные СФЗ, как правило, состоят из средств обнаружения и идентификации противоправных действий, средств сбора, обработки, отображения и передачи тревожных сообщений на соответствующие пульты управления с последующей выдачей с них управляющих воздействий. В процессе функционирования СФЗ реализуется интенсивный информационный обмен, в том числе и обмен конфиденциальной информацией. Любая возможность несанкционированного доступа к информации, циркулирующей в СФЗ, существенно снижает эффективность и надежность использования технических средств физической защиты (ТСФЗ), вплоть до полного снижения функционала СФЗ по обнаружению противоправных действий и адекватного управления ответными действиями. Кроме того, возможность несанкционированного доступа к информационным базам данных СФЗ создает существенные предпосылки к утечке закрытой информации о составе, структуре и решаемых задачах самого объекта защиты. Именно поэтому основополагающими нормативными документами, регулирующими процедуры защиты ряда важных государственных объектов (атомных станций, ядерных установок, объектов переработки и хранения ядерных материалов, крупных энергетических и других потенциально опасных объектов) от преступных посягательств [1–3], предписано обязательное принятие мер по защите информации об организации и функционировании СФЗ.

Таким образом, в связи со стремительным развитием возможностей средств радио и радиотехнической разведки актуальной является задача надежной защиты информации, циркулирующей в СФЗ. Важным элементом такой защиты является комплекс организационно-технических мероприятий по противодействию указанным средствам разведки. Он включает в себя специальные исследования каналов утечки информации, создаваемых ТСФЗ, специальные исследования на объектах, а также аттестационные испытания ТСФЗ, систем и комплексов на их основе на соответствие требованиям безопасности информации.

В настоящее время существуют различные автоматизированные измерительные комплексы, распространяемые на коммерческой основе и позволяющие решать задачи проведения специальных исследований средств вычислительной техники и контроля их защищенности. Анализ их функциональных возможностей, алгоритмов автоматизации действий оператора и программно-технических характеристик показывает следующее:

- существующие автоматизированные комплексы ориентированы на проведение специальных исследований и контроля защищенности только средств вычислительной техники и не приспособлены для исследований каналов утечки информации, создаваемых элементами технических средств физической защиты;
- частотный диапазон большинства комплексов ограничен частотой 1 ГГц, а некоторых — 2 ГГц;
- практически все комплексы используют в качестве измерительного прибора анализатор спектра, что не позволяет проводить измерения слабых сигналов, а также измерения в условиях сложной помеховой обстановки, характерной для объектов, оснащенных системами физической защиты;

- несмотря на то что отдельные комплексы позволяют проводить измерения по нескольким параметрам, все эти параметры являются однотипными и имеют общую природу происхождения;
- все комплексы имеют стандартную структуру: датчик — средство сбора информации — средство обработки информации (ПЭВМ).

Таким образом, с одной стороны, остается нерегламентированным существенный диапазон частот, в котором каналы утечки информации не выявляются и меры по противодействию средствам разведки не предпринимаются, а с другой стороны, отсутствует соответствующее методическое и техническое обеспечение проведения специальных исследований в этом диапазоне. В результате, во-первых, создаются предпосылки для реализации преднамеренного воздействия на СФЗ с целью существенного снижения их функциональных возможностей (вплоть до полного блокирования) и беспрепятственного несанкционированного проникновения на особо опасные объекты, а во-вторых, создаются предпосылки для получения конфиденциальной информации о самом объекте защиты.

В рамках данной публикации кратко изложены основные функциональные возможности более совершенного по сравнению с ближайшими аналогами исследовательского автоматизированного измерительно-регистрирующего комплекса (АИРК).

Основными научно-техническими задачами, решаемыми при разработке АИРК, являлись: сопряжение с помощью шины управления измерительного приемника с антенно-фидерным устройством, поворотной платформой, средствами вычислительной техники и другим необходимым оборудованием, разработка программного обеспечения, учитывающего все требования соответствующих нормативных документов.

В качестве источников первичной информации были выбраны измерительные приемники ведущих зарубежных производителей, обладающие необходимыми для построения АИРК техническими характеристиками. Отечественная измерительная техника с требуемыми характеристиками в настоящее время не производится.

Основными достоинствами разработанного АИРК являются:

1) средства проведения испытаний предусматривают возможность интеграции в единый измерительно-регистрирующий комплекс, работающий в общем информационном пространстве под управлением ПЭВМ и позволяющий проводить измерения и контроль измеряемых параметров в интерактивном режиме. Практически все приборы имеют одинаковый интерфейс связи с ПЭВМ (USB, RS232);

2) основу АИРК составляет рабочая станция — центральный пункт управления (ЦПУ), который, в свою очередь:
- управляет всеми процессами проведения испытаний;
- осуществляет технологический контроль за проведением испытаний;
- протоколирует текущие процессы;
- обеспечивает ведение и поддержание баз данных;
- обрабатывает результаты испытаний и формирует отчетные документы;
- осуществляет планирование проведения испытаний;
- осуществляет контроль работоспособности всех составляющих компонентов макета;

3) программный комплекс ЦПУ обеспечивает:
- занесение кодов идентификаторов в память системы;
- задание характеристик точек доступа;
- установку временных интервалов доступа (окон времени);
- установку уровней доступа для пользователей;
- протоколирование текущих событий;
- ведение и поддержание баз данных;

- регистрацию прохода через точки доступа в протоколе базы данных;
- сохранение баз данных и системных параметров на резервном носителе;
- сохранение баз данных и системных параметров при авариях и сбоях в системе;
- приоритетный вывод информации о нарушениях;
- возможность управления в случае чрезвычайных ситуаций;

4) программное обеспечение ЦПУ устойчиво к случайным и преднамеренным воздействиям следующего вида:

- отключение питания аппаратных средств;
- программный сброс аппаратных средств;
- аппаратный сброс аппаратных средств;
- случайное нажатие клавиш на клавиатуре;
- случайный перебор пунктов меню программы;

5) в составе АИРК организованы автоматизированные рабочие места (АРМ), состав и назначение которых определяются видом воздействующих факторов. Технологическое назначение и задачи, решаемые каждым АРМ, определяются степенью отработки образца, целями испытаний, назначением испытаний, оценочными свойствами испытаний, продолжительностью и интенсивностью их проведения.

Все контрольно-измерительные и регистрирующие компоненты АРМ за счет наличия интерфейсов USB, RS232 объединены в локальную сеть и имеют в своем составе вычислительные средства, управляющие работой сети. Вся дополнительная статистическая информация при необходимости заносится оператором. После завершения испытания результаты передаются в ЦПУ для окончательной обработки.

В состав испытательного оборудования АИРК также могут быть включены приборы, которые принято называть «виртуальными приборами» и которые заменяют ряд приборов их компьютерным представлением либо вообще физически не существуют, но требуются для реализации конкретного испытательного процесса.

Предлагаемый вариант построения АИРК позволяет проводить измерения как медленноменяющихся, так и быстропеременных процессов.

Базовая структура АИРК представлена на рис. 1.

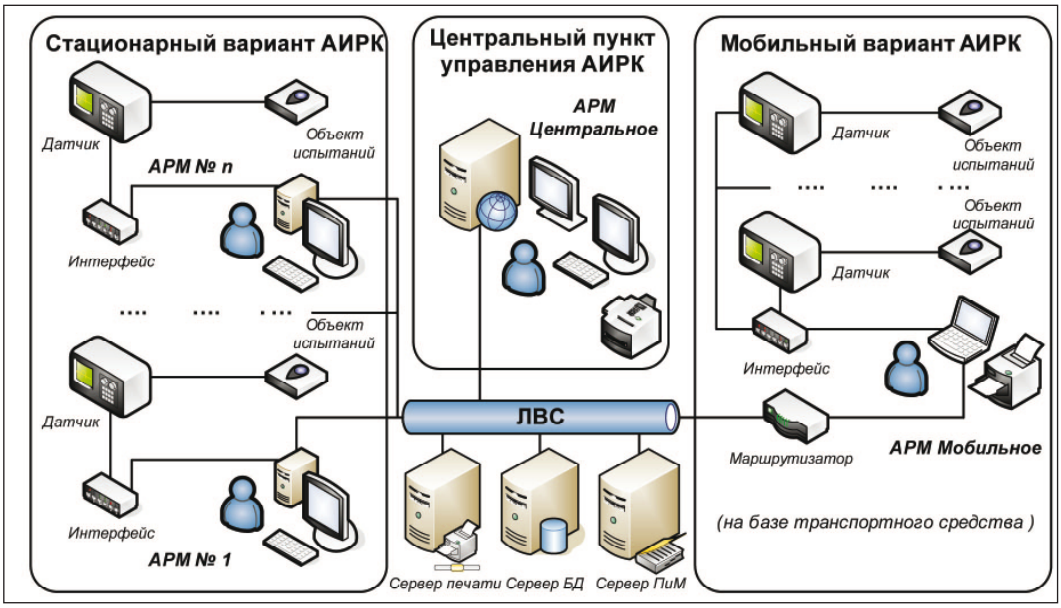

Рис. 1. Базовая структура АИРК

На компьютерах АРМ установлены модули программного обеспечения: интегрированная среда, ПО испытаний, проводимых в режиме реального времени (РВ), локальная база данных и подсистема тарировки. Предусмотрено выполнение функций комплекса:

- конфигурирование и тарировка измерительных трактов;
- создание, изменение, поиск и хранение сценариев испытаний;
- проведение экспериментов, сбор данных и визуализация в реальном масштабе времени;
- послесеансный анализ результатов;
- репликация данных на сервер;
- просмотр результатов в темпе проведения исследований при наличии соответствующего канала связи.

На компьютерах ЦПУ установлена интегрированная среда. Кроме того, на компьютерах ЦПУ может быть установлено программное обеспечение регистрации результатов экспериментов в режиме реального времени. Данный программно-технический комплекс предназначен для регистрации процессов, происходящих при проведении испытаний, и передачи собранной информации во время или после сеанса в базу данных результатов, расположенную на сервере.

На ЦПУ возможно выполнение следующих функций:

- создание, изменение, поиск и хранение сценариев экспериментов;
- послесеансный анализ результатов;
- генерация отчетных документов.

На компьютеры АРМ мобильного АИРК могут быть установлены все модули программного обеспечения: интегрированная среда, ПО испытания РВ, локальная база данных и подсистема тарировки. Возможно выполнение всех функций комплекса, аналогичных функциям АРМ стационарного варианта исполнения АИРК.

Сетевое оборудование АИРК обеспечивает поддержание, функционирование и взаимодействие всех компонентов сети. Данный программно-технический комплекс предназначен для обеспечения связи с компонентами сети и поддержания процессов, происходящих при проведении испытаний, а также для передачи собранной информации во время или после сеанса в базу данных результатов, расположенную на сервере. Базовая структура АРМ АИРК представлена на рис. 2.

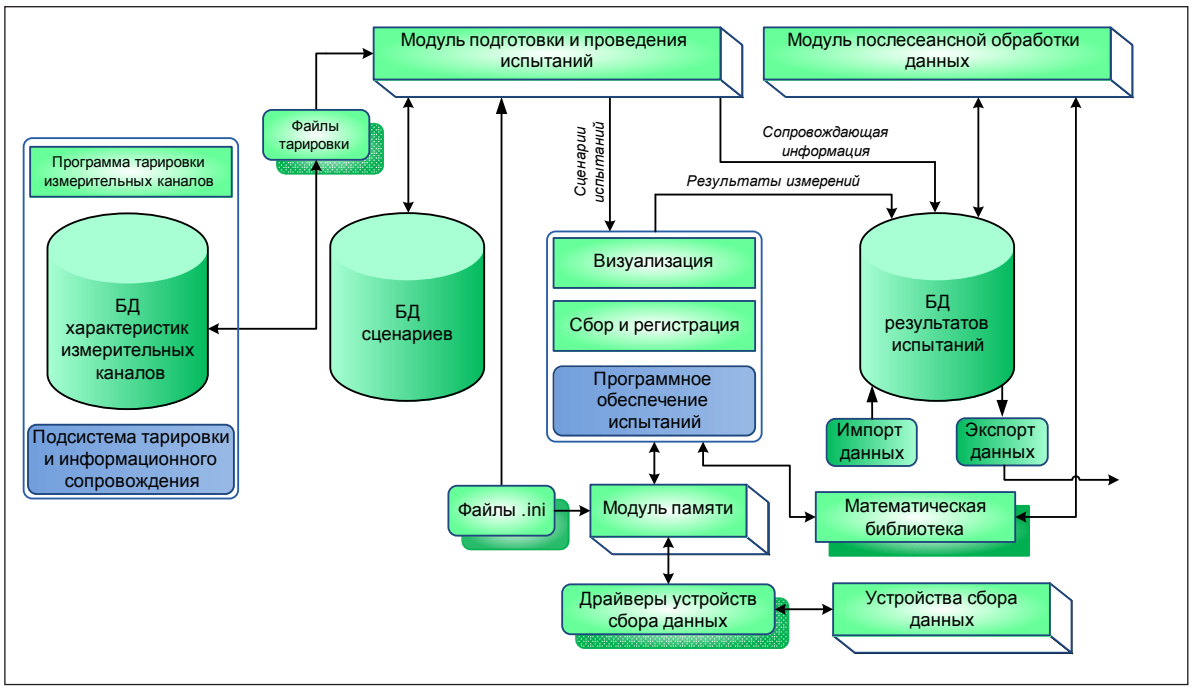

Рис. 2. Базовая структура АРМ АИРК

Комплекс АРМ выполнен по модульному принципу. Основу комплекса АРМ составляет интегрированная среда, позволяющая проводить настройку процесса испытания, поиск нужного сценария в базе данных, запуск программного обеспечения испытаний, просмотр и анализ результатов.

Программное обеспечение испытаний состоит из двух независимых частей, способных работать как единое целое на одном компьютере или поодиночке на отдельных компьютерах.

Подсистема тарировки и информационного сопровождения измерительных каналов передает другим подсистемам комплекса информацию о составе и характеристиках имеющихся измерительных каналов и их элементах, что позволяет формировать измерительные тракты и определять их метрологические характеристики.

Широкое использование технических возможностей ПЭВМ позволяет создавать «виртуальные приборы», функционирующие как на одиночном компьютере и проводящие измерения по отдельному тракту, так и в комплексном режиме измерения ряда параметров с использованием клиент-серверных технологий в рамках распределенной системы сбора и обработки данных. Преимущества этой технологии:

- простота подключения измерительных датчиков широкой номенклатуры к ПЭВМ;
- простое изменение конфигурации процесса испытания;
- высокая надежность оборудования, хорошая диагностика;
- проведение тестирования измерительных трактов перед началом испытаний;
- возможность унификации и гибкость настройки любого сценария испытания и режима измерений;
- гибкая система для решения вопросов метрологического обеспечения и аттестации;
- низкая удельная стоимость оборудования по сравнению с использованием парка различных приборов как отечественного, так и импортного производства.

В ходе разработки АИРК была проведена систематизация нормативно-технической документации (НТД), определены организационно-методические документы, непосредственно регламентирующие проведение испытаний ТСФЗ, систем и комплексов на их основе. Анализ показал, что вся совокупность НТД, связанной с проведением испытаний, разбивается в соответствии с группами однородной продукции ТСФЗ.

Систематизация организационно-методических документов позволяет свести к минимуму усилия по подготовке документов, регламентирующих проведение испытаний ТСФЗ, упрощает подготовку и проведение испытаний, способствует повышению их качества.

Результаты, полученные в ходе выполнения данной работы, позволят в дальнейшем разработать программы и методики испытаний конкретных образцов средств и систем физической защиты с привязкой к необходимым трактам измерений и регистрации АИРК исходя из максимальной ориентации на автоматизированное проведение испытаний с широким использованием средств имитации внешних воздействий.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ.
2. Постановление Правительства РФ от 19 июля 2007 г. № 456 «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов».
3. ГОСТ Р 52860-2007 «Технические средства физической защиты. Общие технические требования».