От редактора

В последние десятилетия в связи с угрозой информационных войн [1] и террористических актов в мировой практике, с одной стороны, активизировалась разработка современных средств технической разведки (СТР), методов ее ведения и возможного прямого воздействия как на информационно-телекоммуникационную инфраструктуру страны, так и на информацию, в частности. С другой стороны, активизировалась и разработка средств противодействия иностранной технической разведке и в том числе средств защиты информации.

Ключевыми задачами в этих условиях являются, во-первых, мониторинг и комплексная оценка электромагнитной обстановки контролируемой зоны с целью противодействия технической разведке иностранного государства (противника), радио- и радиотехнический контроль технических каналов утечки информации, обеспечение электромагнитной совместимости радиоэлектронных средств (РЭС), радиомаскировка. Перечень этих задач объединяется единым понятием «радиоэлектронная защита» (РЭЗ). При этом контролируемой зоной может быть регион, административно-территориальная единица и страна в целом.

В политике защиты информации и, в первую очередь, ее важнейшей составляющей — РЭЗ, весьма актуальной является проблема оценки ее эффективности на основе результатов комплексного технического контроля (КТК) [2, 3]. Это большая, сложная и наукоемкая проблема.

Во-первых, очевидно, техническим контролем должны быть охвачены значительные по территории контролируемые зоны и большое количество контролируемых объектов как ведомственной, так и межведомственной принадлежности. Возникают проблемы их взаимодействия, при организации которого должны рассматриваться технико-технологические, информационные, экономические и правовые аспекты. В этих условиях весьма актуальными становятся задачи регламентации единых правил обмена и обработки информации, унификации программных, технических и программно-технических средств, создание унифицированных рядов комплексов средств автоматизации технического контроля и формирование защищенного информационного пространства зоны обслуживания пользователей систем (ведом-

ственной или межведомственной принадлежности) КТК РЭС (далее для краткости изложения — ЕИП).

Во-вторых, сложность реализации КТК РЭС (далее для краткости КТК). Она определяется теми особенностями, которые характерны для КТК и которые определяются его многоцелевой направленностью, многообразием функциональных задач, выполняемых средствами КТК и, наконец, требованиями к вероятностно-временным показателям и требованиями к условиям применения.

Чтобы показать эту взаимосвязь, целесообразно в краткой форме изложить цели и основные функциональные задачи КТК.

Цели КТК:

- определение достаточности и эффективности мероприятий КТК по противодействию СТР иностранного государства;
- выявление и обеспечение закрытия технических каналов утечки конфиденциальной информации;
- выявление и принятие мер по устранению нарушений установленных режимов и порядка использования РЭС и радиочастотного спектра.

Основные задачи КТК:

- мониторинг выполнения установленных требований (норм) и контроль запланированных мероприятий по РЭЗ от СТР иностранных государств;
- контроль достаточности и эффективности РЭЗ от утечки по техническим каналам;
- контроль выполнения установленных порядка и правил использования РЭС — потенциальных источников непреднамеренных радиопомех важнейшим РЭС;
- проведение специальных исследований, сертификации, технической экспертизы и паспортизации категорированных объектов;
- оперативное информирование должностных лиц органов управления (ДЛ ОУ) о результатах КТК и выявленных нарушениях для принятия соответствующего решения.

Многоцелевая направленность технического контроля с точки зрения разнообразия контролируемых объектов от отдельных РЭС до критически важных объектов (КВО), включая «мобильные критические объекты» — места проведения массовых мероприятий населением, предопределяет проведение разных видов технического контроля.

В общем случае КВО — объект, нарушение (или прекращение) функционирования которого приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или

существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени.

Многообразие методов и средств технической разведки и связанная с этим *многоплановость функциональных задач*, решаемых системой КТК для достижения поставленных целей, регламентируют порядок и условия применения средств КТК. Технический контроль может проводиться или на контролируемом объекте, или внутри контролируемой зоны, или из-за пределов контролируемой зоны. Следовательно, средства КТК должны быть наземного (переносного, мобильного, стационарного), воздушного и космического применения.

Система КТК должна удовлетворять весьма жестким требованиям по своевременности, достоверности и надежности доведения результатов контроля объектов до лиц, принимающих решения (ЛПР) по проведению мероприятий, направленных на недопущение или сокращение до минимума ущерба от воздействия деструктивных факторов на защищаемые сведения.

Кроме того, для повышения эффективности функционирования системы КТК, должна быть создана автоматизированная система управления и мониторинга (АСУМ) средствами КТК и системой КТК в целом.

Регламентация требований применения средств КТК касается, прежде всего, возможности их применения в любое время суток, года и в любых природных зонах.

Важнейшими факторами, определяющими выполнение жестких требований к системе КТК, являются использование последних достижений науки и техники в области информационных и телекоммуникационных технологий, средств вычислительной техники, программных средств, средств измерений и телекоммуникаций.

Таким образом, КТК направлен на мониторинг электромагнитной обстановки, оценку степени РЭЗ на контролируемом объекте и/или в пределах контролируемой зоны в интересах информационной поддержки ДЛ ОУ по определению достаточности средств и сил КТК и принятия решения по проведению эффективных мероприятий по противодействию СТР иностранного государства.

Особенности функционирования современных систем КТК:

- появление новых радио- и радиотехнических систем и средств связи и радиоэлектронной борьбы;
- расширение частотного диапазона;
- применение новых видов сигналов с широкой базой и новых видов модуляции;
- работа иностранных систем и средств в непосредственной близости к контролируемым объектам (например, Интернет);

- усложнение электромагнитной обстановки.

Авторы книги не стремились изложить все аспекты проблемы защиты информации и ее контроля во всей их широте, глубине и многообразии, а остановились только на тех вопросах, которые связаны с проблемой КТК эффективности РЭЗ.

Поскольку в печатной продукции недостаточно информации, а по некоторым направлениям в рассматриваемой предметной области отсутствует полностью, авторы, не претендуя на законченность исследований, сделали попытку восполнить существующий пробел и внести посильный вклад в решение этой важной проблемы.

Это касается, прежде всего, теоретического обоснования основных положений, связанных с формированием ЕИП КТК, технико-технологическими принципами создания как ведомственных, так и межведомственных систем КТК, разработкой межведомственного профиля протоколов взаимосвязи открытых систем межведомственной системы КТК, определением порядка разработки комплекса стандартов с регламентацией понятий в рассматриваемой предметной области.

Для решения этих глобальных проблем определены платформы ЕИП и проведен анализ их параметров, признаков и составляющих. Под платформой понимается совокупность средств определенного вида, необходимых для создания и/или безопасного функционирования и развития инфраструктуры ЕИП. Средствами, обеспечивающими создание и/или безопасное функционирование и развитие инфраструктуры ЕИП, могут быть методы, правила, процедуры, нормы, а также нормативные документы, средства информатизации, автоматизации, связи, защиты информации и КТК.

Предпосылкой определения перечня платформ являются базовые условия формирования ЕИП. По замыслу, перечень платформ является функционально полным и не избыточным инструментарием реализации таких аспектов создания информационного пространства, которые обеспечат его единство и защищенность.

Рассмотрены вопросы радио-, радиотехнического и специального контроля, оценки и обеспечения ЭМС радиоэлектронных систем и средств.

Формирование информационно-телекоммуникационной инфраструктуры ЕИП проведено на основе профилей базовых стандартов (стандартизованных протоколов) взаимосвязи открытых систем. Показано, что профиль протоколов выполняет функции системного интегратора при создании единой информационно-телекоммуникационной среды.

Проведен анализ традиционных методов измерений параметров технического контроля, методов и видов испытаний систем КТК и их элементов.

Создание унифицированных платформ ЕИП в значительной степени зависит от понятийного аппарата, обеспечивающего взаимопонимание между разработчиками, изготовителями и заказчиками элементов инфраструктуры ЕИП. Поэтому в монографии этому вопросу уделено внимание в виде разработки широкого перечня взаимоувязанных терминологических статей на основе использования понятийной модели.

Книга базируется на результатах исследований, выполненных авторами в качестве руководителей и исполнителей НИР, реализованных в ОКР в области создания автоматизированных комплексов КТК, автоматизированных измерительных комплексов, автоматизированных пунктов управления и серийно выпускаемых, а также в области создания нормативно-технической базы.

Книга предназначена для широкого круга специалистов в области КТК РЭС. Результаты работы могут найти применение в научно-исследовательских институтах, на предприятиях и организациях промышленности, в системах органов заказчиков систем и средств КТК РЭС. Книга может быть использована в качестве учебного пособия в профильных вузах страны.

Доктор технических наук,
профессор *А.А. Сахнин*

Введение

Переход информации в разряд важнейших ресурсов человечества ведет к неизбежному возникновению проблемы обладания этим ресурсом и, как следствие, его защиты, тем более, что развитие наукоемких технологий, к числу которых можно отнести информационные и телекоммуникационные технологии, всегда было связано с укреплением обороноспособности государства. Поэтому защита информации в этой сфере — важнейшее направление политики государства.

Возрастающая роль защиты информации вызвана также ведением в современную эпоху так называемых информационных войн, когда без существенных материальных затрат по сравнению с традиционными войнами можно одержать победу информационным оружием.

Все эти обстоятельства требуют пристального внимания к защите конфиденциальной информации, несанкционированный доступ к которой может привести к тяжелым невосполнимым утратам в сфере экономики страны и ее обороноспособности.

В этих условиях очевидную стратегическую значимость приобретает комплексный технический контроль (КТК) радиоэлектронных средств.

Масштабы, сложность и методы КТК определяются разнообразием средств технической разведки иностранного государства (противника), а также характеризуются разнообразием таких его видов, как радио- и радиотехнический контроль, контроль утечки информации по техническим каналам, акустический, гидроакустический, инфракрасный, фотографический, визуально-оптический, оптико-электронный и другие виды контроля, и жесткими требованиями по своевременности, достоверности и надежности его проведения.

Основными объектами технического контроля являются критически важные объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени.

В монографии рассматривается путь формирования защищенного информационного пространства зоны обслуживания пользователей систем КТК. Причем этот путь предусматривает решение таких основополагающих задач, как установление базовых требований к

информационно-телекоммуникационной инфраструктуре единого информационного пространства (ЕИП) КТК, формирование его облика в составе концептуальной модели, архитектурной основы и совокупности платформ. Решение каждой из этих проблем носит комплексный характер, а объединяющим методологическим принципом их реализации является системный подход.

Ключевым звеном в формировании ЕИП КТК определена платформа нормативно-технического обеспечения, регламентирующая единое нормативное поле для всех разработчиков, в границах которого закладываются технико-технологические основы создания средств, комплексов информатизации, автоматизации, связи, радиоэлектронной защиты, технического контроля и их взаимосвязи в рамках информационно-телекоммуникационной инфраструктуры ЕИП КТК.

В монографии отражены концептуальные основы построения системы КТК РЭС, при этом особое внимание уделено созданию автоматизированной системы управления и мониторинга (АСУМ), которая направлена на эффективное поддержание и использование ресурсов системы КТК при формировании в интересах должностных лиц КТК организационного, оперативно-технического и технологического трактов управления техническим контролем.

Впервые комплексно рассмотрены пути решения крупных и сложных взаимосвязанных и взаимодополняющих задач разработки единой информационно-телекоммуникационной среды технического контроля, которая обеспечивает лицам, принимающим решения, предоставление услуг в любой точке контролируемой территории в режиме реального масштаба времени. Роль «системного интегратора» при этом отведена ведомственному профилю протоколов взаимосвязи открытых систем, поскольку он, по определению, регламентирует логику функционирования компонентов инфраструктуры ЕИП КТК и обеспечивает реализацию функций взаимосвязи его пользователей.

Разработанные в монографии методологические основы формирования ЕИП КТК, технико-технологические принципы построения системы КТК и АСУМ могут быть положены в основу создания межведомственной системы КТК и разработки таких фундаментальных документов, как:

- «Концепция формирования межведомственного защищенного информационного пространства КТК РЭС»;
- концепция «Единая автоматизированная межведомственная система КТК РЭС»;
- концепция «Единая АСУМ межведомственной системы КТК РЭС»;
- «Профиль протоколов взаимосвязи открытых систем «Единой автоматизированной межведомственной системы КТК РЭС».

Предложенная методология может быть использована при планировании поэтапного развития и эволюционного совершенствования инфраструктуры ЕИП РФ на основе унифицированного ряда комплексов средств автоматизации технического контроля, отвечающего требованиям мониторинга информационной безопасности как в масштабе всей страны, так и в интересах различных ведомств, включая силовые ведомства, используя при этом дифференцированный подход к обеспечению безопасности информации с учетом внутриведомственных требований.