Введение

С начала третьего тысячелетия происходит жестокое столкновение двух парадигм мироустройства: однополярной, не предусматривающей суверенитетов, — с одной стороны, и полицентричной, с многими суверенными центрами, — с другой [1]. Одновременно усиливается мировая конкуренция за ресурсы [2]. На этом фоне с учетом стремительного развития инфокоммуникационных технологий главной формой межгосударственной борьбы стало информационное противоборство.

Одним из многих доказательств этого являются сенсационные разоблачения Викиликса об использовании западными спецслужбами популярных устройств и сервисов для негласного получения информации о действиях владельцев [3]. Проблемой для информационной безопасности (ИБ) могут стать социальные сети, теневой Интернет, криптовалюты, хакерство.

Информационная сфера стала пятой сферой вооруженной борьбы после суши, моря, воздушного и космического пространства. США первыми в 2009 г. признали наличие у себя отдельного рода войск — кибервойск численностью около 10 тысяч человек. Затем кибервойска стали заводить у себя другие армии. В 2014 г. в российских Вооруженных Силах созданы командование и войска информационных операций [4].

Таким образом, уклад жизни человечества и геополитический ландшафт в XXI веке изменились настолько сильно, что руководство России вынуждено обновлять документы стратегического планирования. Так, в декабре 2016 г. Президент России В.В. Путин утвердил новую Доктрину информационной безопасности Российской Федерации [5], а в мае 2017 г. — новую Стратегию развития информационного общества в РФ [6] на 2017—2030 гг. Эти стратегические документы определяют приоритетные национальные интересы в информационной сфере: добиться технологического прорыва и информационного суверенитета, а также обеспечить высокое качество подготовки пригодных для этого кадров.

Главными драйверами грядущего технологического прорыва в информационной сфере как условия информационного суверенитета России являются:

- обеспечение нацеленности технического регулирования в информационной сфере на высокий научно-технологический уровень инфокоммуникаций (ИК),
- обеспечение высокой точности оценки соответствия ИК требованиям технических регламентов,
- удовлетворение растущего спроса рынка труда на инженеров-новаторов с безупречной фундаментальной подготовкой.

Учебное пособие призвано раскрыть эти связанные между собой инструменты развития ИК на ближайшие десятилетия. Опыт многих лет убедил авторов, что знания стандартов и методов измерения соответствия не являются избыточными, а, напротив, очень нужны выпускникам направлений «ИБ» и «Электроника, радиотехника и системы связи» в работе. Полезно им также знать образовательные и профессиональные стандарты (ПСт) как ориентиры в процессе обучения.

Учебное пособие посвящено 10-летию кафедры «Безопасность радиосвязи» Московского технического ордена Трудового Красного Знамени университета связи и информатики. Вклад авторов в подготовку учебного пособия распределился следующим образом: Ю.А. Родичев — главы 1, 3, раздел 2.3, научное редактирование; Ю.А. Кубанков — введение, разделы 2.1, 2.2, 4.1, заключение; П.И. Симонов — разделы 4.2, 4.3. В разделах 1 и 3 используется материалы Ю.А. Родичева из ряда его трудов [7, 8, 9, 10].

Учебное пособие может представлять интерес для аспирантов и студентов, обучающихся по направлениям «ИБ» и «Электроника, радиотехника и системы связи», а также для всех специалистов, связанных с безопасностью ИК.