DOI: 10.24411/1993-8314-2019-10018

А. Ю. Юршев, *канд. техн. наук, АО «ИнфоВотч», г. Москва, ay@infowatch.com*
М. Б. Смирнов, *АО «ИнфоВотч», г. Москва, ms@infowatch.com*

Методика и результаты тестирования совместимости средств защиты информации и АСУТП

В настоящее время отсутствуют необходимые методики для комплексной оценки совместимости средств защиты информации (СЗИ) и АСУТП, которые необходимы при проектировании систем безопасности объектов критической информационной инфраструктуры. Предложена методика оценки совместимости СЗИ и АСУТП с применением программ и методик проведения перекрестных испытаний, используемых при приемке таких систем. Получены практические результаты по оценке совместимости средств защиты информации с АСУТП различных производителей.

Ключевые слова: средство защиты информации, оценка соответствия, совместимость, испытания, информационная безопасность, критическая информационная инфраструктура, АСУТП.

Введение

В 2018 г. в Российской Федерации сформирована нормативно-правовая база по обеспечению безопасности критической информационной инфраструктуры (КИИ). Основой базы стал Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры» [8]. К указанному закону изданы уже 16 подзаконных актов.

Объекты критической информационной инфраструктуры — это информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС), автоматизированные системы управления (АСУ) субъектов критической информационной инфраструктуры, а субъекты критической информационной инфраструктуры — это государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности; российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [8].

В соответствии с постановлением Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня по-