Предисловие

Задачи обеспечения информационной безопасности в современном мире приобретают огромное значение по причинам все большего проникновения информационных технологий в жизнь общества и роста угроз экономике и безопасности от возможных потерь, к которым может привести намеренное или ненамеренное нарушение функционирования как отдельных устройств, так и информационной инфраструктуры на локальном или даже глобальном уровнях.

Важнейшим направлением исследований и разработок, которые призваны сократить риски реализации таких угроз, является создание специальных средств защиты информации и построения защищенных систем, которые, в первую очередь, нацелены на защиту и обеспечение надежной и бесперебойной работы элементов критической инфраструктуры страны. Одним из ключевых элементов инфраструктуры любой программной системы является операционная система, поскольку она лежит в основании программного стека в любом программном комплексе.

В 2013 году компания АО «НПО РусБИТех», которая уже более 10 лет производит и внедряет специальные защищенные версии операционной системы (ОС) семейства Linux — операционную систему специального назначения (ОССН) Astra Linux Special Edition, предложила объединить усилия специалистов из двух, достаточно далеких в то время областей исследований для решения практической задачи — выведения специальной операционной системы на самый высокий уровень требований к обеспечению защиты информации, который определяется современными российскими и международными стандартами. С этой целью была сформирована группа из специалистов по информационной безопасности (под руководством проф. П.Н. Девянина) и специалистов ИСП РАН, имеющих опыт как в теоретических вопросах формальной верификации программных моделей, так и в применении различных техник верификации к крупным программным системам, в том числе к различным ОС общего назначения и реального времени.

Изначально было ясно, что придется параллельно решать научные, методические и технические задачи проекта и координировать исследовательские работы с планами АО «НПО РусБИТех» по подготовке к сертификации новых версий ОССН. Такая координация

одновременно затрудняла систематическое развитие методов, инструментов моделирования и верификации и помогала выявлять наиболее сложные, практически значимые задачи в контексте проблем верификации и сертификации большого программного продукта.

За счет тесной интеграции исследовательских и практических работ к настоящему времени удалось разработать комплекс методик и их инструментальную поддержку, что, в свою очередь, позволило внедрить результаты этих работ в процесс производства и сертификации ОССН и осенью 2017 года получить сертификат ФСТЭК России на соответствие ОССН требованиям профиля защиты ОС общего назначения (типа «А») второго класса защиты [1–3]. Это первый и пока единственный в России опыт сертификации ОС общего назначения в соответствии с требованиями такого высокого уровня.

Данная монография является плодом коллективного труда. При ее написании активно использовались материалы статей авторов по отдельным вопросам. Достаточно много времени пришлось уделить вопросам согласования терминологии и структуры изложения, так как описывается не отдельная научная проблема, а достаточно сложный процесс, состоящий из нескольких этапов работ, на каждом их которых используются разные методы и разные инструменты. Описанный процесс не является эталоном, он может пересматриваться и оптимизироваться в том или ином измерении, его можно позиционировать как «референсный», т. е. его внедрение позволяет утверждать, что концепция строгого и даже формального подхода к построению политики безопасности управления доступом таких крупных систем, как ОС общего назначения, реализуема. Кроме того, референсный процесс в дальнейшем можно использовать как некоторую базу для сравнения и выбора при решении отдельных задач, возникающих в процессах производства и сертификации защищенных программных систем.

Авторы выражают благодарность компании «Акционерное общество «НПО РусБИТех» за постоянную поддержку данной работы. Особенно важный вклад в работу внес заместитель начальника департамента этой компании А.Л. Оружейников, который на протяжении всего этого времени осуществлял решение сложных задач координации работ, определения приоритетов и предоставления необходимой технической документации на ОССН.

Также необходимо отметить важный вклад сотрудников ИСП РАН М.У. Мандрыкина (развитие инструментов дедуктивной верификации Си-программ) и Н.Ю. Комарова (верификация компонентов механизма безопасности в ядре ОССН).

Неоценимое влияние на работу оказал академик В.П. Иванников, который до последних дней следил за ходом работ, увлекал своим энтузиазмом и торопил с решением центральных проблем верификации сложнейших механизмов защиты современных ОС.