Предисловие

Дисциплины «Защита в операционных системах» и «Безопасность в операционных системах» являются основными при подготовке специалистов по защите информации. Находясь на стыке теории и практики, эти дисциплины позволяют обеспечить успешное освоение обучающимися нескольких профессиональных и профессионально-специализированных компетенций, а в дальнейшем расширить полученные знания и умения при изучении методов и технологий защиты информации в компьютерных сетях, системах управления базами данных и др.

Рассматриваемые дисциплины в целом обеспечены необходимой учебной литературой [34]. Однако многолетний опыт и сложившаяся практика преподавания этих дисциплин показывают, что помимо изучения общих подходов к обеспечению безопасности операционных систем (ОС), сопровождаемого, несомненно, полезным их иллюстрированием примерами из ОС различных семейств (*Microsoft Windows*, *Linux*, *Android*, *MacOS* и др.), целесообразен глубокий, детальный анализ некоторой конкретной востребованной защищённой ОС, который бы позволил обучающимся не фрагментарно, а системно составить представление о рассматриваемой области знаний. Кроме того, взятый в Российской Федерации курс на импортозамещение с принятием Правительством Российской Федерации решения об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд [27], создаёт предпосылки к тому, что спектр защищённых ОС, которые будут применяться в автоматизированных системах органов государственной власти и предприятий промышленности, не будет слишком широким.

Аналогичная ситуация складывается при преподавании дисциплины «Модели безопасности компьютерных систем», являющейся чрезвычайно важной для формирования у обучающихся знаний об используемых в теории информационной безопасности научных подходах. Эта дисциплина также обеспечена учебной литературой [11], однако приводимые в ней примеры из практики разработки механизмов безопасности управления доступом и информационными потоками различных компьютерных систем не в полной мере позволяют

показать обучающимся, что в современных условиях возможен не только теоретический анализ отдельных частных задач по защите информации в компьютерных системах, а возможна реализация законченного комплексного научно-обоснованного решения по созданию защищённой ОС.

В целом полезно отметить, что разработка защищённой ОС — сложный наукоемкий процесс, требующий концентрации усилий многих отечественных центров компетенции в области теории и практики информационной безопасности. В ряде случаев неудачи при создании таких ОС являлись следствием неспособности их разработчиков обеспечить, во-первых, сопровождение и развитие ОС, её необходимую функциональность, а во-вторых, обосновать, в том числе строго научно, что реализованные для защиты ОС технические решения действительно позволяют достичь заданных целей безопасности.

В связи с этим разработка отечественной защищённой операционной системы специального назначения (ОССН) *Astra Linux Special Edition* [23, 61] изначально велась путём сочетания усилий специалистов по созданию механизмов защиты ОС и представителей научного сообщества [14]. ОССН является в настоящее время единственной в Российской Федерации отечественной ОС, сертифицированной во всех трёх системах сертификации средств защиты информации (МО, ФСТЭК и ФСБ России), на её основе созданы и внедрены в органах исполнительной власти, на предприятиях промышленности сотни автоматизированных систем в защищённом исполнении, в том числе обеспечивающих защиту информации с грифом до «совершенно секретно» включительно. Впервые в отечественной практике разработки подобных систем в качестве научной основы для создания механизмов защиты ОССН, начиная с версии 1.4, была использована современная теоретическая модель — мандатная сущностно-ролевая ДП-модель безопасности управления доступом и информационными потоками в ОС семейства *Linux* (сокращённо МРОСЛ ДП-модель) [11].

По этим причинам ОССН была выбрана в качестве предмета для научного анализа и практического освоения при изучении дисциплин «Защита в операционных системах», «Безопасность в операционных системах» и «Модели безопасности компьютерных систем», и ей посвящено настоящее учебное пособие.

Пособие состоит из четырёх глав, в первой из которых анализируется понятие защищённой ОС, делается обзор таких ОС, принадлежащих семейству *Linux*. Кроме того, в главе рассматриваются основные элементы архитектуры ОССН, а также приёмы пользова-

тельской работы и администрирования, не затрагивающие принципиально новые механизмы защиты, построенные на основе МРОСЛ ДП-модели и реализованные в ОССН, начиная с версии 1.4.

Во второй главе приводятся основные элементы МРОСЛ ДП-модели, в том числе используемые для описания состояний рассматриваемой в её рамках абстрактной системы. Излагаются заданные в модели требования к реализации мандатного и ролевого управления доступом и мандатного контроля целостности, в том числе приводятся примеры основанных на их выполнении де-юре и де-факто правил преобразования состояний. Формулируются условия безопасности системы в смыслах мандатного контроля целостности, Белла–ЛаПадулы и контроля информационных потоков по времени. Анализируется способы обоснования корректности реализации модели в программном коде ОССН, а также подходы к адаптации и внедрения модели в ОССН.

В третьей главе детально рассматриваются результаты практической разработки механизмов защиты ОССН, начиная с версии 1.4, основанных на реализации элементов МРОСЛ ДП-модели. В том числе анализируются механизмы мандатных управления доступом и контроля целостности, управления доступом к объектам графической подсистемы ОССН, особенности аутентификации и аудита, реализации сетевого взаимодействия и доменной инфраструктуры. Описываются типовые приёмы по администрированию перечисленных механизмов защиты.

Для практического закрепления знаний и навыков, полученных при изучении пособия, в четвёртой главе приводится лабораторный практикум по администрированию ОССН. Для каждой из входящих в него лабораторных работ указывается её цель, время на выполнение, краткие теоретические сведения, используемое методическое и лабораторное обеспечение, порядок выполнения, содержания отчёта и контрольные вопросы.

Настоящее учебное пособие будет полезно преподавателям и обучающимся (бакалаврам, специалистам, магистрам, аспирантам и адъюнктам) по направлению «Информационная безопасность», а также специалистам в области разработки или анализа безопасности защищённых ОС.