Предисловие

Дисциплины «Защита операционных систем» и «Безопасность операционных систем» 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 [59]. 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 (ПО), происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд [50], включением в рамках национального проекта «Цифровая экономика Российской Федерации» в План мероприятий по федеральному проекту «Информационная безопасность» [88] задач по обеспечению преимущественного использования отечественного ПО государственными органами, органами местного самоуправления и организациями, создаёт предпосылки к тому, что спектр защищённых сертифицированных ОС, которые будут применяться в автоматизированных системах (АС) 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 [17], 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, т. е. продемонстрировать требуемый уровень доверия к ОС как средству защиты информации.

В связи с этим разработка АО «НПО РусБИТех» отечественной защищённой операционной системы специального назначения (ОССН) *Astra Linux Special Edition* [100, 101] изначально велась путём сочетания усилий специалистов по созданию механизмов защиты ОС и представителей научного сообщества [18]. ОССН является в настоящее время единственной в Российской Федерации отечественной ОС, сертифицированной во всех трёх системах сертификации средств защиты информации (Минобороны, ФСТЭК и ФСБ России). При этом она стала первой сертифицированной ФСТЭК России на соответствие требованиям профиля защиты ОС общего назначения (типа «А») второго класса защиты [61], что является пока единственным в России опытом сертификации ОС общего назначения на соответствие требованиям такого высокого уровня.

На основе ОССН созданы и внедрены в органах исполнительной власти, на предприятиях промышленности тысячи автоматизированных систем в защищённом исполнении (АСЗИ), 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) [17].

По этим причинам ОССН была выбрана в качестве предмета для научного анализа и практического освоения при изучении дисциплин «Защита операционных систем», «Безопасность операционных систем» 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 пользовательской работы и администрирования, не затрагивающие принципиально новые механизмы защиты, построенные на основе МРОСЛ ДП-модели и имеющиеся в ОССН, начиная с версии 1.4, и полнофункционально реализованные, начиная с версии 1.6.

Во второй главе приводятся основные элементы МРОСЛ ДП-модели в её иерархическом представлении [21, 22], в том числе используемые для описания состояний рассматриваемой в её рамках абстрактной системы. Излагаются заданные в модели требования ролевого управления доступом (в отличие от [33] в базовый уровень ролевого управления доступом МРОСЛ ДП-модели добавлены запрещающие роли), мандатного контроля целостности и мандатного управления доступом, 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 (скрытых каналов) по времени. Анализируются подходы к адаптации и внедрению модели при разработке механизмов защиты ОССН.

В третьей главе детально рассматриваются результаты практической разработки механизмов защиты ОССН, основанных на внедрении элементов МРОСЛ ДП-модели, акцентируя внимание на полнофункциональную реализацию этих механизмов, начиная с версии 1.6. 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 на базе *Astra Linux Directory* (*ALD*) и проекта *FreeIPA* [68], ряда дополнительных функций безопасности (замкнутая про-

граммная среда, запрет установки бита исполнения и блокировка интерпретаторов, запрет исполнения данных, очистка освобождаемых областей на жёстком диске, контроль целостности (неизменности) файлов, управление доступом к подключаемым устройствам). 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 девяти входящих в него лабораторных работ приводятся ее цель, время на выполнение, краткие теоретические сведения, используемое методическое и лабораторное обеспечение, порядок выполнения, содержание отчёта и контрольные вопросы.

Таким образом, настоящее третье издание учебного пособия по сравнению с его вторым изданием [4] существенно дополнено и актуализировано, во-первых, для адаптации его материалов к изменениям механизмов защиты ОССН версии 1.6, во-вторых, для учёта новых результатов, полученных при научном сопровождении разработки ОССН, в-третьих, для доработки его материалов на основе полученного методического опыта преподавания по тематике ОССН в рамках образовательных программ высшего образования и повышения квалификации. Кроме того, часть материалов второго издания учебного пособия, посвящённых осуществляемым совместно сотрудниками АО «НПО РусБИТех» и Института системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН) работам по верификации МРОСЛ ДП-модели вплоть до её непосредственной реализации в программном коде ОССН в контексте выполнения утверждённых ФСТЭК России «Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» [83], исключены из третьего издания пособия, так как для подробного освещения этих вопросов была издана монография [33].

Настоящее учебное пособие будет полезно преподавателям и обучающимся (бакалавриатам, специалистам, магистрантам, аспирантам и адъюнктам) по укрупненной группе специальностей и направлений подготовки (УГСНП) «Информационная безопасность», а также специалистам по защите информации, в особенности в области разработки и анализа безопасности защищённых ОС.

1 Обеспечение безопасности операционных систем семейства Linux

1.1. Понятие защищённой (доверенной) операционной системы

Существуют два основных подхода к трактовке понятия защищённой автоматизированной системы (АС), применимых к операционным системам (ОС). Первый подход подразумевает, что защищённость ОС обеспечивается при реализации некоторых заданных изначально (например, в соответствующих стандартах или руководящих документах [9, 61, 83]) требований по безопасности, включая наличие некоторого набора механизмов защиты, проверку отсутствия предопределённого перечня уязвимостей и т. п. При втором подходе рассматривается возможность использования ОС в составе АС, которые считаются их владельцами (пользователями) критическими, в связи с чем в ОС должен обеспечиваться комплекс средств защиты информации (СЗИ), адекватный угрозам безопасности именно этих систем. На первый взгляд, эти два подхода не противоречат друг другу, так как вряд ли в критических АС будут применяться решения, не реализующие хотя бы минимальные требования по безопасности. Вместе с тем ОС при выполнении всех требований по безопасности может быть контролируема извне, например её разработчиком. В указанных условиях второй подход подразумевает, что под защищёнными подразумеваются решения, которые в англоязычной литературе обозначаются термином *trusted*, или, в отечественной интерпретации — доверенные.

Таким образом, защищённой (доверенной) целесообразно считать ОС, которая не только реализует заданные априорно требования безопасности, но и адекватна угрозам безопасности, специфичным для отечественных АС, в том числе для которой отсутствует возможность несанкционированного влияния на её работу извне, при этом владелец (пользователь) защищённой ОС должен иметь однозначное представление об алгоритме функционирования её защитных механизмов во всех режимах работы.

Это требование становится все более актуальным в последние годы. Автоматическое обновление, автоматическое оповещение разработчиков о программных ошибках, разнообразные онлайн-сервисы существенно повышают потребительские качества прикладного и системного программного обеспечения ОС, но, с другой стороны, создают все больше возможностей для производителей ПО, в том числе ОС, контролировать действия пользователей [98, 126]. Для целого ряда применений защищённых ОС вопрос доверия к её разработчику оказывается более значимым, чем вопрос об объёме и качестве реализации в данной ОС стандартных механизмов обеспечения безопасности.

Именно этими соображениями можно объяснить рост интереса к отечественным защищённым ОС, отмечающийся в последнее время в Российской Федерации со стороны органов государственной власти и предприятий промышленности. Дополнительным стимулом по данному направлению стало принятое Правительством Российской Федерации решение об установлении запрета на допуск ПО, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд [50], планируемое «законодательное закрепление норм, обеспечивающих преференции для компьютерного, серверного и телекоммуникационного оборудования и ПО отечественного производства при осуществлении закупок для государственных и муниципальных нужд, а также при предоставлении различных форм государственной поддержки» [88]. Высказываются прогнозы, что в случае утверждения и принятия Программы развития российского сегмента сети Интернет «к 2025 году все государственные учреждения и стратегические предприятия будут оснащены компьютерами на российской элементной базе с отечественной операционной системой на борту» [62].

В современных условиях перспективная отечественная защищённая ОС должна отвечать следующим требованиям:

- соответствовать требованиям обеспечения технологической независимости (импортозамещения) Российской Федерации в важнейших областях информатизации, телекоммуникации и связи;
- быть пригодной к функционированию в компьютерных сетях, как изолированных, так и подключённых к сети Интернет (или иным телекоммуникационным сетям), в том числе ориентированных на обработку информации, отнесённой к государственной тайне, или персональных данных;
- реализовывать современные механизмы обеспечения информационной безопасности, учитывающие возможность обработки в