Предисловие

Во многих информационных системах, их средствах защиты информации (СЗИ), особенно являющихся многопользовательским распределенным системным программным обеспечением (ПО), например операционными системами (ОС) или системами управления базами данных (СУБД), реализуются политики управления доступом [13]. Это могут быть распространенные политики дискреционного, мандатного, ролевого управления доступом, мандатного контроля целостности, возможно также атрибутивного, типизированного, каких-то других видов управления доступом или политики, сочетающие несколько его видов. Как правило, реализующий политики управления доступом механизм защиты является базовым для обеспечения безопасности, во многом определяющим функциональность других механизмов СЗИ. При этом чаще всего, как во многих ОС, это будет механизм дискреционного управления доступом или, например, как в ОС семейства *Microsoft Windows*, сочетание дискреционного управления доступом и мандатного контроля целостности, реже, как в ОС *Astra Linux* (операционной системе специального назначения *Astra Linux Special Edition*) [32, 47], сочетание дискреционного и мандатного управления доступом с мандатным контролем целостности. В СУБД, как правило, используется ролевое управление доступом.

Изначально с начала 70-х годов прошлого столетия для научных исследований используемых в СЗИ технологий и механизмов управления доступом разрабатывались соответствующие формальные модели (это были рассмотренные в учебном пособии модели Белла–ЛаПадулы, *Take-Grant*, Харрисона–Руззо–Ульмана и др.). Впоследствии по мере накопления практики их применения при создании, анализе защищенности и обосновании доверия к СЗИ требования к представлению их описаний стали включаться в нормативные документы и стандарты в области защиты информации.

Первым примером здесь являлся опубликованный в 1985 г. стандарт TCSEC («Оранжевая книга») [89], в котором в класс защиты B2 было включено требование к описанию формальной модели управления доступом (*formal model of the security policy*). В дальнейшем аналогичные требования включались в большинство профильных стандартов, в том числе в ГОСТ Р ИСО/МЭК 15408-3 (*ISO/IEC* 15408-3) [7], в котором была задан компонент доверия *ADV_SPM*.1 «Формальная модель политики безопасности». В этом компоненте доверия без раскрытия подробных требований к описанию формальной модели было указано, что оно должно быть изложено в формальном стиле (с использованием, например, математического языка), должно быть определено понятие «безопасность» и представлено формальное доказательство того, что анализируемое СЗИ (в терминах этого стандарта — объект оценки) не может перейти в небезопасное состояние.

В Российской Федерации критерии, которым должны отвечать описания формальных моделей управления доступом, рекомендации по их разработке и верификации закреплены в семействе профильных национальных стандартов ГОСТ Р 59453 «Защита информации. Формальная модель управления доступом» [13–16].

Вместе с тем разработка формальной модели управления доступом как комплексный многоэтапный процесс может вызывать значительные трудности, особенно в случае, когда она необходима для моделирования СЗИ, являющегося сложным системным ПО, ОС или СУБД. Это связано с тем, что для обеспечения адекватности формальной модели такому СЗИ, возможности ее применения в качестве основы для разработки его механизмов защиты, доказательства выполнения им условий безопасности требуются существенная детализация и усложнение формальной модели. В противном случае выводы, полученные при анализе безопасности СЗИ в рамках формальной модели, и она сама могут оказаться бесполезными, далекими от реальных условий функционирования СЗИ.

В связи с этим детальное изучение формальных моделей управления доступом целесообразно по следующим основным причинам.

Во-первых, формальные модели могут быть использованы для анализа безопасности существующих или перспективных СЗИ, особенно в случаях, когда требуется обеспечить доверие к их защищенности. Так, согласно нормативным документам

ФСТЭК России, требования по разработке модели безопасности СЗИ, реализующего политики управления доступом, изложены в «Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» [3] и «Методике выявления уязвимостей и недекларированных возможностей в программном обеспечении» [36].

Во-вторых, существующие формальные модели могут быть использованы как основа (как «строительный материал») или, согласно рекомендациям ГОСТ Р 59453.4–2025 [16], как базовые модели для разработки более совершенных моделей, позволяющих более точно описывать и исследовать особенности функционирования механизмов защиты современных систем.

В-третьих, часто классические формальные модели позволяют анализировать свойства механизмов защиты, которые уже были хорошо известны из опыта их практической разработки или эксплуатации. В то же время по мере развития теории информационной безопасности могут создаваться новые модели, с применением которых возможны сначала теоретическое описание и исследование свойств механизмов защиты, а уже затем подтверждение наличия этих свойств у реальных систем.

В-четвертых, владение знаниями о формальных моделях управления доступом предоставляет специалисту в области информационной безопасности возможности для строгого научного и теоретически обоснованного изложения результатов прикладных исследований, что, в свою очередь, создает дополнительные предпосылки для его научного роста.

В существующей литературе по информационной безопасности и кибербезопасности, в том числе учебной, часто приводятся описания формальных моделей управления доступом. Однако их изложение, как правило, носит фрагментарный характер. При этом основное внимание уделяется лишь общей формулировке основных определений и результатов моделей либо краткому их перечислению обзорного характера (без подробного рассмотрения, применяемого математического аппарата и приведения доказательств). В то же время в книгах, где доказательства приводятся, они, как правило, даются в общих чертах.

В учебном пособии рассмотрены с полными доказательствами положения классических формальных моделей: дискреционного, мандатного, ролевого управления доступом, мандатного контроля целостности, безопасности информационных потоков

и изолированной программной среды. Приведен используемый в рассматриваемых моделях математический аппарат. Классические модели дополнены семейством моделей безопасности управления доступом и информационными потоками (сокращенно — ДП-моделей), адаптированных к условиям функционирования современных систем. В том числе в пособии описываются элементы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства *Linux* (сокращенно — МРОСЛ ДП-модели), на основе которой строится механизм управления доступом в отечественной защищенной ОС *Astra Linux*, уже много лет сертифицируемой по самым высоким классам защиты и уровням доверия [32, 47]. МРОСЛ ДП-модель демонстрирует возможности современных подходов к моделированию и теоретическому анализу безопасности защищенных систем таких, как ОС или СУБД, и включает реализацию востребованных в таких системах мандатных управления доступом и контроля целостности совместно с перспективным ролевым управлением доступом.

Кроме того, в учебном пособии приведены контрольные вопросы и задачи, среди которых выделены задачи повышенной сложности (они отмечены символом «*»), даны примеры решения задач на практических занятиях, а также в каждой главе пособия изложены методические рекомендации по организации изучения моделей. В первую очередь эти рекомендации нацелены на использование преподавателями, так как они включают дополнительные разъяснения сложных для обучающихся моментов доказательств теоретических результатов, иллюстрации применения этих результатов в реальных защищенных системах, примеры решения задач на практических занятиях, используемые при этом схемы и рисунки. Кроме того, эти рекомендации будут полезны обучающимся, желающим глубже разобраться в соответствующей теории, а также для их более эффективной подготовки к учебным занятиям.

Настоящее учебное пособие базируется на 3-м издании учебного пособия «Модели безопасности компьютерных систем» [29], от которого отличается корректировкой содержания с учётом накопившегося методического опыта, в том числе дополнением пособия главой 7, в которой проанализировано профильное семейство национальных стандартов ГОСТ Р 59453 [13–16], приведением используемой в пособии терминологии в соответствие с этими стандартами, а также актуализацией описания элемен-

тов МРОСЛ ДП-модели с учётом результатов её развития, верификации и реализации на её основе собственных механизмов управления доступом ОС *Astra Linux*.

Учебное пособие разработано на основе тридцатилетнего опыта преподавания формальных моделей управления доступом в ряде образовательных организаций Федерального учебно-методического объединения по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ), в том числе в ИКСИ Академии ФСБ России, РТУ МИРЭА и МГТУ им. Н.Э. Баумана.