Предисловие

Освоение знаний о технологиях, реализованных в программных средствах защиты информации (СЗИ), навыков их применения играет большую роль в образовательном процессе по направлению «Информационная безопасность». В особенности, когда речь идет о СЗИ, имеющих широчайший спектр практического применения и часто являющихся фундаментом большинства соответствующих комплексных решений. В первую очередь к числу таких программных СЗИ относятся операционные системы (ОС).

В этой связи изучению вопросов защиты информации в ОС уделяют большое внимание как в рамках соответствующих профильных дисциплин (например, «Защита в операционных системах», «Безопасность операционных систем» и др.) образовательных программ высшего образования, так и при освоении программ дополнительного профессионального образования. Находясь на стыке теории и практики, эти дисциплины позволяют обеспечить успешное освоение обучающимися нескольких общепрофессиональных компетенций, а в дальнейшем расширить полученные знания и умения при изучении методов и технологий защиты информации в компьютерных сетях, системах управления базами данных (СУБД) и др. При этом с учетом сложности архитектуры и функциональности ОС, которые применяются, начиная с небольших устройств и заканчивая облачными инфраструктурами, методически они являются достаточно сложным объектом для преподавания и изучения.

Кроме того, особую актуальность тематика защиты информации в ОС обретает в настоящее время, когда взятый Российской Федерацией курс на технологическую независимость и обеспечение безопасности критической информационной инфраструктуры привел к значительному росту числа информационных систем органов государственной власти, корпораций, предприятий промышленности, построенных с применением отечественных решений и технологий. Ключевую роль здесь конечно

играют ОС, сертифицированные для использования в указанных информационных системах.

Среди таких операционных систем следует отметить созданную ООО «РусБИТех-Астра» (ГК «Астра») ОС специального назначения (ОССН) *Astra Linux Special Edition* [1, 16], являющуюся единственной ОС, сертифицированной во всех трёх российских системах сертификации СЗИ (Минобороны, ФСТЭК и ФСБ России), а также в системе сертификации Республики Беларусь. При этом ОССН сертифицирована ФСТЭК России на соответствие требованиям профиля защиты ОС общего назначения (типа «А») первого класса защиты (уровня доверия), что также является единственным опытом сертификации ОС общего назначения на соответствие требованиям высшего уровня. Поэтому широкое внедрение ОССН в отечественных информационных системах, очевидная потребность подготовки для этого квалифицированных пользователей и администраторов ОССН, разработчиков приложений для нее мотивировали авторов на подготовку настоящего учебного пособия.

Целесообразно отметить, что состав применяемых в сертифицированных ОС общего назначения, включая ОССН, механизмов защиты достаточно разносторонен. Он включает средства аудита, идентификации и аутентификации, управления доступом, фильтрации информационных потоков и др. [17]. Это объясняется необходимостью таким ОС, как СЗИ, противостоять в реальных информационных системах самым разным атакам нарушителя.

Не менее обширен состав методов и технологий (например, статический и динамический анализ программного кода, формальное моделирование политик управления доступом и др.), используемых для достижения доверия к ОС согласно ГОСТ Р 56939-2016 [5] и основанным на нем нормативным документам ФСТЭК России [2, 15]. Особенно, когда как в случае с ОССН все перечисленное требуется для обеспечения соответствия высшим уровням доверия. Это, с одной стороны, позволяет говорить о формировании и апробации на примере ОССН методологии разработки безопасного системного ПО [14], а с другой стороны, несомненно оказывает влияние на разработку, эксплуатацию и администрирование ОССН.

Однако, в отличие от [1], рассматриваемая в настоящем учебном пособии тематика сужена только до вопросов, раскрываю-

щих особенности реализации и администрирования в ОССН механизма управления доступом. Это сделано по следующим причинам. Во-первых, в ОССН этот механизм создает основу для всей ее архитектуры защиты. Во-вторых, в этом механизме внедрены оригинальные, не имеющие аналогов в ОС семейства Linux технологии, такие, как мандатный контроль целостности и мандатное управление доступом, уверенное владение которыми во многом обеспечивает эффективные применение и администрирование ОССН в целом. В-третьих, при разработке механизма управления доступом ОССН была изначально применена мандатная сущностно-ролевая ДП-модель безопасности управления доступом и информационными потоками в ОС семейства *Linux* (сокращённо МРОСЛ ДП-модель) [11], которая по сути стала первой из использованных при создании ОССН технологий обеспечения доверия. В последующих частях пособия планируется раскрыть вопросы, касающиеся других механизмов защиты ОССН.

Структура настоящего учебного пособия сформирована с учетом того, что, начиная с релиза 2021 г., ОССН поставляется в виде единого дистрибутива, способного функционировать в одном из трех режимов работы подсистемы безопасности (уровне защищенности): «Базовом», «Усиленном» или «Максимальном».

Функциональные возможности уровня защищенности «Базовый» («Орел») в части механизмов защиты основаны на штатном для ОС семейства *Linux* дискреционном управлении доступом. Поэтому этот уровень защищенности подходит для работы с общедоступной информацией в информационных системах различных организаций, а также для защиты информации в государственных информационных системах (ГИС) 3-го класса защищенности, информационных системах персональных данных (ИС ПД) 3–4-го уровней защищенности и значимых объектов критической информационной инфраструктуры (КИИ) 3-й категории.

Уровень защищенности «Усиленный» («Воронеж») в первую очередь включает механизмы мандатного контроля целостности (МКЦ) и замкнутой программной среды (ЗПС). Этот уровень предназначен для обработки и защиты информации ограниченного доступа, не составляющей государственную тайну, в том числе в ГИС, ИС ПД и на значимых объектах КИИ любого класса (уровня) защищенности (категории значимости).

Уровень защищенности «Максимальный» («Смоленск») реализует мандатное управление (разграничение) доступом (МРД) и обеспечивает защиту информации, содержащей государственную тайну любой степени секретности, и предназначен для обработки информации любой категории доступа в ГИС и ИС ПД, в составе значимых объектов КИИ, в иных информационных (автоматизированных) системах, обрабатывающих информацию ограниченного доступа, в том числе содержащую сведения, составляющие государственную тайну до степени секретности «особой важности» включительно.

При этом в целом выбор уровня защищенности ОССН осуществляется, исходя из реальных угроз (модели нарушителя) для конкретной информационной системы, оценки возможности противостоять этим угрозам с помощью механизмов защиты выбранного уровня защищенности. Например, реализованные в ОССН, начиная с уровня защищенности «Усиленный» («Воронеж»), механизмы МКЦ и ЗПС позволяют эффективно предотвращать атаки с применением эксплойтов и компьютерных вирусов.

Согласно трем уровням защищенности ОССН первые три главы учебного пособия посвящены каждому из них. Кроме того, в первой главе дополнительно описан механизм расширения дискреционного управления доступом «Киоск-2», а во второй — статического контроля целостности (неизменности) файлов и замкнутой программной среды. При этом завершающий параграф каждой из трех глав раскрывает особенности представления в рамках МРОСЛ ДП-модели соответствующего уровню защищенности механизма управления доступом — дискреционного управления доступом, мандатного контроля целостности и мандатного управления доступом.

Для практического закрепления знаний и навыков, полученных при изучении пособия, в четвёртой главе приводится лабораторный практикум по настройке и администрированию рассмотренных в предыдущих главах механизмов защиты ОССН. Для каждой из десяти входящих в него лабораторных работ указываются её цель, сведения, необходимые для выполнения работы, и порядок ее выполнения.

Настоящее учебное пособие будет полезно преподавателям и обучающимся (бакалаврам, специалистам, магистрантам и аспирантам) по направлению «Информационная безопасность», слу-

шателям и преподавателям профильных программ дополнительного профессионального образования, а также специалистам по защите информации, в особенности в области разработки и анализа безопасности защищённых ОС.