# Предисловие к третьему изданию

Исследование формальных моделей, особенно моделей безопасности управления доступом и информационными потоками в компьютерных системах (КС), создаёт предпосылки для развития теории информационной безопасности и разработки новых эффективных методов анализа защищенности современных или перспективных КС, например операционных систем (ОС), СУБД, средств виртуализации.

При этом информационная безопасность — одна из наиболее динамично развивающихся современных наук, скорость обновления её знаний чрезвычайно высока. Теоретические результаты, ещё несколько лет назад признававшиеся адекватными уровню развития применяемых для защиты КС технологий, сегодня могут оказаться безнадёжно устаревшими. Яркий пример этого — рассматриваемая в учебном пособии классическая модель Белла–ЛаПадулы, долгое время являвшаяся основой построения защищённых КС с мандатным управлением доступом. Хотя неоднократно было показано (например, в [15, 16]), что эта модель не предоставляет механизмов защиты от запрещённых информационных потоков (скрытых каналов) по времени [8, 9] от сущностей с высоким уровнем конфиденциальности к сущностям с низким уровнем конфиденциальности.

В связи с этим детальное изучение моделей безопасности КС целесообразно по следующим основным причинам.

Во-первых, модели могут быть непосредственно использованы для анализа безопасности существующих или перспективных КС особенно в случаях, когда требуется обеспечить доверие к защищенности таких КС. Например, согласно вступившим в силу с 1 июня 2019 г. [24] утверждённым приказом ФСТЭК России от 30 июля 2018 г. № 131 «Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» разработка формальной модели управления доступом и ее верификация с применением инструментальных средств [23] стали частью требований соответственно 4 и 3 уровней доверия, на которые ориентируются многие отечественные разработчики сертифицированных средств защиты информации. Ещё ранее в соответствии с [4] в профилях защиты и заданиях по безопасности, включающих

оценочный уровень доверия 6 и 7 (ОУД 6 и ОУД 7) или непосредственно компоненту доверия ADV_SPM.1 «Формальная модель политики безопасности», также требовалось, чтобы при разработке КС была использована формальная модель политики безопасности.

Во-вторых, существующие модели безопасности КС могут быть использованы как основа (как «строительный материал») для разработки более совершенных моделей, позволяющих более точно описывать и исследовать особенности функционирования механизмов защиты современных КС.

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

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

В существующей литературе по информационной безопасности, в том числе учебной, часто приводятся описания моделей безопасности. 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 моделей безопасности КС: дискреционного, мандатного, ролевого управления доступом, безопасности информационных потоков и изолированной программной среды. Приведён используемый в рассматриваемых моделях математический аппарат. Классические модели дополнены семейством моделей безопасности логического управления доступом и информационными потоками (сокращённо, ДП-моделей), адаптированных к условиям функционирования современных КС. В том числе в пособии опи-

сывается некоторые элементы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства *Linux* (сокращённо, МРОСЛ ДП-модели), на основе которой строится механизм управления доступом в отечественной защищённой операционной системе специального назначения (ОССН) *Astra Linux Special Edition* [1, 46], уже много лет сертифицируемой по самым высоким классам защиты, в том числе по требованиям безопасности информации к ОС общего назначения (типа «А») 1 класса защиты в системе сертификации средств защиты информации ФСТЭК России [34]. МРОСЛ ДП-модель демонстрирует возможности современных подходов к моделированию и теоретическому анализу безопасности защищённых КС и включает реализацию востребованных в таких КС 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 защищённых КС, 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.

В целом содержание учебного пособия основано на реализации компетентностного подхода, положенного в основу федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) третьего поколения в области информационной безопасности. В том числе учебное пособие направлено на методическое обеспечение дисциплины «Модели безопасности компьютерных систем», являющейся одной из основных в специальности 10.05.01 «Компьютерная безопасность», освоение которой формирует у обучающихся следующие общепрофессиональные и профессиональные компетенции:

- способен разрабатывать формальные модели политик безопасности, политик управления доступом и информационными по-

токами в компьютерных системах с учетом угроз безопасности информации;

- способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.

При этом изучение моделей безопасности КС основано на дисциплинах вида: «Информатика», «Основы информационной безопасности», «Математическая логика и теория алгоритмов», «Дискретная математика», «Основы построения защищённых операционных систем», «Защита программ и данных», знания и практические навыки, полученные при изучении моделей, обеспечивают освоение дисциплин вида: «Основы построения защищённых сетей», «Основы построения защищённых СУБД», а также могут использоваться обучающимися при разработке выпускной квалификационной работы.

Учебное пособие разработано на основе двадцатипятилетнего опыта преподавания моделей безопасности в ряде образовательных организаций Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ), в том числе в ИКСИ Академии ФСБ России.

# 1 Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем

## 1.1. Элементы теории информационной безопасности в рамках субъект-сущностного подхода

### 1.1.1. Основные научные направления теории информационной безопасности

Каждому научному направлению или подходу в теории информационной безопасности соответствует, как правило, самостоятельная система понятий. Поэтому прежде чем приводить определения самих понятий дадим краткую характеристику этих направлений и подходов, акцентировав внимание на те из них, которые будут наиболее близки к рассматриваемым в учебном пособии моделям безопасности.

Научным подходом, на основе которого базируется моделирование безопасности КС, является **субъект-сущностный подход** (ранее он назывался субъект-объектным подходом) [47, 49, 56]. Он зародился одним из первых в теории информационной безопасности, в его рамках исследуемая КС представляется в виде абстрактной системы (автомата), каждое состояние которой описывается доступами, реализуемыми субъектами к сущностям (объектам или контейнерам), а переходы КС из состояния в состояние описываются командами или правилами преобразования состояний, выполнение которых, как правило, инициируется субъектами. Этому подходу будет посвящено фактически все учебное пособие.

Направление **моделирование компьютерных атак, распределенных многоагентных систем обнаружения вторжений** получило в настоящее время существенный импульс для своего развития, в том числе в результате принятых решений о создании и эксплуатации государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) [3, 38]. Теории, используемые в рамках этого направления, как правило, существенно

отличаются от субъект-сущностного подхода и базируется в основном на применении теории вероятностей, нейронных сетей, иммунных систем для исследования компьютерных атак, сетевой активности, выявления в ней аномалий или злоупотреблений [58, 61].

Другим актуальным направлением теории информационной безопасности стало **применение методов верификации** для автоматизации проверки корректности реализации политик безопасности, сетевых протоколов, программного кода [25, 26, 30]. При этом изначально акцентировалось внимание на поиск в них типовых ошибок, а при верификации программного кода типовых «программистских» ошибок, например некорректной обработки длин буферов данных или символьных строк при их копировании и т. п.

Однако по мере разработки рассматриваемой в учебном пособии мандатной сущностно-ролевой ДП-модели безопасности управления доступом и информационными потоками в операционных системах семейства *Linux* (МРОСЛ ДП-модели) и реализации её в отечественной защищённой ОССН *Astra Linux Special Edition* [1, 46] получил развитие подход, ориентированный на перевод модели в формализованную нотацию *Event-B* (*Rodin Platform*), что позволило верифицировать описание модели и осуществить дедуктивные доказательства её свойств [19, 23, 53].

После чего на основе формализованного представления модели с использованием инструмента дедуктивной верификации кода *Why3* (в среде разработки *Frama-C*) были заданы спецификации (предусловия и постусловия) функций механизма управления доступом ОССН и проверено их выполнение, что позволило обосновать адекватность реализации модели непосредственно в программном коде. Таким образом, субъект-сущностный подход и направление применения методов верификации оказались тесно взаимоувязанны в процессе разработки отечественной защищённой ОССН и получения научно обоснованных гарантий её безопасности.

Кроме того, разработка и верификация с применением инструментальных средств формальной модели управления доступом являются частью утверждённых ФСТЭК России «Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» [24].

Четвёртое направление, включающее **технологии и методы повышения безопасности разработки программного обеспечения**, в первую очередь основанные на применении различных способов его тестирования, включая тестирование по методу «за-

шумления» (*fuzzing*) [35], так же как второе направление базируется на собственной аксиоматике, не связанной напрямую с субъект-сущностным подходом и выходит за рамки настоящего учебного пособия.

### 1.1.2. Сущность, субъект, доступ, информационный поток

В теории информационной безопасности, как правило, используются понятия «сущность» (*entity*), «объект» (*object*), «субъект» (*subject*) и «доступ» (*access*). Для описания свойств КС, в которых рассматриваются сущности, обладающие внутренней структурой, в ряде случаев, кроме понятия «объект», рассматривается понятие «контейнера» (*container*).

Любая сущность КС в произвольный момент времени может быть однозначно представлена набором данных, которое может рассматриваться как состояние сущности.

На основе [4] дадим определения.

**Определение 1.1.** Объект или контейнер — сущность КС, которая содержит или получает информацию (данные) и над которой субъекты выполняют операции. Субъект — активный компонент КС, инициирующий выполнение операций над сущностями. При этом по определению предполагается:

- контейнеры могут состоять из объектов и других контейнеров;
- субъекты КС могут получать доступ к объектам целиком, но не могут получать доступ к частям объекта;
- субъекты КС могут получать доступ к контейнеру и к сущностям, из которых состоит контейнер.

Для выполнения операций над сущностями КС субъекты осуществляют к ним доступы. В большинстве случаев рассматриваются следующие основные виды доступов:

- *read* — доступ на чтение из сущности;
- *write* — доступ на запись в сущность;
- *append* — доступ на запись в конец данных, описывающих состояние сущности;
- *execute* — доступ на активизацию субъекта из сущности.

Другие виды доступов субъектов к сущностям КС часто могут быть реализованы с использованием рассмотренных видов доступов.

В основе рассматриваемого субъект-сущностного подхода используется аксиома 1.1 [78], позволяющая выделить элементы КС, необходимые для анализа её безопасности.

**Аксиома 1.1 (основная аксиома информационной безопасности).** В рамках субъект-сущностного подхода все вопросы

безопасности информации в КС описываются доступами субъектов к сущностям.

Важную роль при исследовании безопасности КС играет анализ информационных потоков (*information flow*), возникающих в результате реализации субъектами КС доступов к сущностям. В соответствии с [40, 52] дадим определение.

**Определение 1.2.** Информационным потоком от сущности-источника (субъекта-источника) к сущности-приёмнику (субъекту-приёмнику) называется преобразование данных в сущности-приёмнике, реализуемое субъектами КС, зависящее от данных, содержащихся в сущности-источнике.

В рассматриваемых в учебном пособии формальных моделях анализ безопасности информационных потоков основан на применении аксиом 1.1–1.3.

**Аксиома 1.2.** Все действия в КС, в том числе выполнение операций над сущностями, порождение информационных потоков, изменение параметров и настроек системы защиты КС, порождение новых субъектов, могут быть инициированы только субъектами КС с использованием доступов к сущностям КС.

**Аксиома 1.3.** Все информационные потоки в КС порождены доступами субъектов к сущностям.

### 1.1.3. Классическая классификация угроз безопасности информации

В соответствии с [7] дадим определение.

**Определение 1.3.** Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

При классификации угроз выделяют три основных свойства безопасности информации в КС [5].

**Определение 1.4.** Конфиденциальность информации — обеспечение доступа к информации только авторизованным пользователям.

**Определение 1.5.** Целостность информации — обеспечение достоверности и полноты информации и методов её обработки.

**Определение 1.6.** Доступность информации — обеспечение доступа к информации и связанным с ней активам авторизованным пользователям по мере необходимости.

Таким образом, под информационной безопасностью в первую очередь понимается защита её конфиденциальности, целостности и

доступности, при этом также может требоваться обеспечение её аутентичности, подотчётности, неотказуемости и надёжности [6].

В соответствии с тремя основными свойствами безопасности информации различают три классических угрозы безопасности информации в КС.

**Определение 1.7.** Угроза конфиденциальности информации состоит в нарушении установленных ограничений на доступ к информации только авторизованным пользователям.

**Определение 1.8.** Угроза целостности информации — несанкционированное изменение информации или методов её обработки.

**Определение 1.9.** Угроза доступности информации — несанкционированное блокирование доступа к информации авторизованным пользователям (блокирование может быть постоянным или на некоторое время, достаточное, чтобы информация стала бесполезной).

Кроме перечисленных угроз часто выделяют ещё одну угрозу безопасности информации в КС, реализация которой, как правило, предшествует осуществлению любой из классических угроз.

**Определение 1.10.** Угроза раскрытия параметров КС — преодоление защиты КС, выявления параметров, функций и свойств её системы безопасности.

При анализе угрозы целостности информации и моделировании соответствующих механизмов управления доступом следует иметь в виду, что язык её описания часто аналогичен языку описания угрозы конфиденциальности. Используя при формулировании требований защиты информации от угрозы целостности доступы субъектов к сущностям, можно сделать выводы аналогичные выводам, полученным при описании требований защиты от угрозы конфиденциальности, при этом следует заменить доступы на чтение информации доступами на запись и наоборот.

Условия реализации угрозы доступности информации могут быть заданы с использованием параметра, называемого максимальным временем ожидания ответа на запрос на доступ к ресурсу (*MWT — maximum wait time*). Таким образом, для каждого ресурса КС определяется время, приемлемое для ожидания его получения.

### 1.1.4. Виды информационных потоков

Как правило, при моделировании безопасности КС [47, 49, 55] рассматриваются два основных вида информационных потоков: информационный поток по памяти и информационный поток по времен. В современных КС велико многообразие способов реализации