"ГОСТ Р 59453.3-2025. Национальный стандарт Российской Федерации. Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке" (утв. и введен в действие Приказом Росстандарта от 10.03.2025 N 111-ст)

Утвержден и введен в действие
Приказом Федерального
агентства по техническому
регулированию и метрологии
от 10 марта 2025 г. N 111-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАЩИТА ИНФОРМАЦИИ

ФОРМАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

ЧАСТЬ 3

РЕКОМЕНДАЦИИ ПО РАЗРАБОТКЕ

**Information protection. Formal access control model.
Part 3. Recommendations on development**

ГОСТ Р 59453.3-2025

ОКС 35.030

**Дата введения
31 марта 2025 года**

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Институтом системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН), Обществом с ограниченной ответственностью "РусБИТех-Астра" (ООО "РусБИТех-Астра"), Федеральным автономным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФАУ "ГНИИИ ПТЗИ ФСТЭК России")

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 "Защита информации"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 10 марта 2025 г. N 111-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. N 162-ФЗ "О стандартизации в Российской Федерации". Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе "Национальные стандарты", а официальный текст изменений и поправок - в ежемесячном информационном указателе "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее

уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя "Национальные стандарты". Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

Введение

Реализация политик управления доступом, как правило, является одной из основных функций, выполняемых средствами защиты информации. Разработка и описание для этого формальных моделей управления доступом позволяет обеспечить доверие к таким средствам защиты информации, уменьшить число недостатков при их проектировании (моделировании, разработке). При этом описания формальных моделей управления доступом должны соответствовать критериям, установленным ГОСТ Р 59453.1-2021, и быть верифицированы согласно рекомендациям ГОСТ Р 59453.2-2021.

Вместе с тем разработка формальных моделей управления доступом в большинстве случаев является комплексным многоэтапным процессом, от качества выполнения которого зависит возможность демонстрации соответствия их описаний моделируемым средствам защиты информации и обеспечения уверенности в корректности реализации этими средствами политик управления доступом.

В связи с этим настоящий стандарт устанавливает рекомендации по разработке и описанию формальных моделей управления доступом.

1 Область применения

Настоящий стандарт устанавливает рекомендации по разработке и описанию формальных моделей управления доступом, на основе которых разрабатываются средства защиты информации, реализующие политики управления доступом.

Настоящий стандарт предназначен для разработчиков средств защиты информации, реализующих политики управления доступом, а также для органов по сертификации и испытательных лабораторий при проведении сертификации средств защиты информации, реализующих политики управления доступом.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 59453.1 Защита информации. Формальная модель управления доступом. Часть 1. Общие положения

ГОСТ Р 59453.2 Защита информации. Формальная модель управления доступом. Часть 2. Рекомендации по верификации формальной модели управления доступом

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю "Национальные стандарты", который опубликован по

состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя "Национальные стандарты" за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1

абстрактный автомат: Изложенная формально модель дискретного устройства, описываемого входным и выходным алфавитами, множеством состояний, функцией переходов из состояний в состояния и функцией выходов.

Примечание - При описании формальных моделей управления доступом, как правило, применяются абстрактные автоматы без выхода. В математике в качестве таких автоматов определяются абстрактные автоматы, описание которых не включает выходной алфавит и функцию выходов.

[ГОСТ Р 59453.1-2021, пункт 3.1]

3.2

верификация формальной модели управления доступом: Подтверждение посредством представления объективных свидетельств непротиворечивости формальной модели управления доступом и выполнения заданных в ее рамках условий безопасности.

[ГОСТ Р 59453.2-2021, пункт 3.1]

3.3 **иерархическое представление формальной модели управления доступом:** Представление формальной модели управления доступом, при котором ее описание разбивается на несколько слоев (уровней), где каждый последующий слой наследует, а при необходимости корректирует или дополняет элементы предыдущего слоя.

3.4

информационный поток: Преобразование информации в объекте или субъекте доступа, зависящее от информации в объекте или субъекте доступа, реализуемое субъектом(ами) доступа.

Примечание - Объект или субъект доступа, в котором при создании информационного потока преобразуется информация, как правило, называют

приемником информационного потока, объект или субъект доступа, от информации в котором зависит это преобразование, - источником информационного потока, субъект(ы) доступа, реализующий информационный поток, - инициатором(ами) информационного потока.

[ГОСТ Р 59453.1-2021, пункт 3.2]

3.5

информационный поток по памяти: Информационный поток, основанный на использовании памяти, в которую реализующий его субъект(ы) доступа записывает или откуда считывает информацию.

Примечание - Память, используемая для создания информационного потока по памяти, может являться объектом доступа (например, когда такой памятью является файл) или не являться объектом доступа (например, когда такой памятью является сегмент стека процесса операционной системы). При этом источником или приемником такого информационного потока могут являться объекты или субъекты доступа.

[ГОСТ Р 59453.1-2021, пункт 3.3]

3.6 **информационный поток по времени:** Информационный поток, при реализации которого передающий субъект доступа модулирует передаваемой информацией некоторый изменяющийся во времени процесс, а субъект доступа, принимающий информацию, ее демодулирует, при этом фактор времени является существенным.

3.7

скрытый канал: Информационный поток, который может быть применен для нарушения политик управления доступом.

[ГОСТ Р 59453.1-2021, пункт 3.12]

3.8 **сокращенная формальная модель управления доступом:** Формальная модель управления доступом, полученная из другой формальной модели путем либо использования только части ее описания, либо задания в этом описании дополнительных ограничений.

3.9

формальная модель (управления доступом): Математическое или формализованное (машиночитаемое, пригодное для автоматизированной обработки) описание средства защиты информации и компонентов среды его функционирования, предоставление доступов между которыми регламентируется политиками управления доступом, реализуемыми этим средством защиты информации.

[Адаптировано из ГОСТ Р 59453.1-2021, пункт 3.21]

4 Общие положения

4.1 Рекомендации настоящего стандарта по разработке формальной модели управления доступом, на основе которой разрабатывается средство защиты информации, реализующее политики управления доступом, направлены на обеспечение соответствия описания формальной модели критериям, установленным ГОСТ Р 59453.1.

4.2 Рекомендуются следующие этапы разработки и описания формальной модели управления доступом:

- определение границ моделирования средства защиты информации;

- определение видов политик управления доступом, рассматриваемых при моделировании и реализуемых средством защиты информации;

- выбор технологий, инструментальных средств (при необходимости) и практических приемов разработки формальной модели;

- описание формальной модели;

- описание и доказательство выполнения условий безопасности, в том числе при верификации формальной модели.

4.3 На этапе определения границ моделирования средства защиты информации, реализующего политики управления доступом, рекомендуется зафиксировать используемые при этом ограничения, допущения или исключения, при этом показать их влияние на снижение сложности описания формальной модели при обеспечении его соответствия моделируемому средству защиты информации. В том числе следует зафиксировать:

- назначение формальной модели для существующего или проектируемого средства защиты информации, наличие или отсутствие возможности внесения изменений в средство защиты информации согласно разрабатываемой формальной модели.

Примечание - Разработка формальной модели для проектируемого средства защиты информации или такого средства, в режимы функционирования которого могут вноситься изменения, предоставляет больше возможностей для моделирования, так как подразумевает при этом меньше ограничений, накладываемых не подлежащими изменению режимами функционирования этого средства. Вместе с тем моделирование существующего средства защиты информации позволяет получить больше данных об особенностях его функционирования и, как следствие, более точно отразить их в формальной модели;

- политики управления доступом, реализуемые средством защиты информации и регламентирующие предоставление доступов между всеми компонентами среды функционирования средства защиты информации или только их подмножеством.

Примечание - Моделирование средства защиты информации, реализующего политики управления доступом, регламентирующие предоставление доступов между всеми компонентами среды его функционирования, является, как правило, более сложным. Вместе с тем оно позволяет более точно отразить в описании формальной модели режимы функционирования такого средства, например в части условий возникновения информационных потоков;

- существенные особенности среды функционирования средства защиты информации (наличие сетевой инфраструктуры, применение технологий виртуализации или другие особенности), учитываемые при разработке формальной модели.

Примечание - Учет всех особенностей среды функционирования средства защиты информации может значительно затруднить моделирование, при этом не оказав существенного влияния на обеспечение соответствия описания формальной модели этому средству. Например, моделирование управления доступом в операционной системе без явного учета ее возможного использования в сетевой инфраструктуре может не оказать негативного влияния на свойства разработанной формальной модели, при этом существенно упростить ее описание.

4.4 При определении рассматриваемых при моделировании видов реализуемых средством защиты информации политик управления доступом рекомендуется использовать политики, определенные в ГОСТ Р 59453.1 (политики дискреционного управления доступом, мандатного контроля целостности, мандатного управления доступом и ролевого управления доступом). Необоснованное расширение состава рассматриваемых видов политик управления доступом может сказаться на сложности моделирования, формулирования и доказательства выполнения условий безопасности, в том числе при верификации формальной модели. Сокращение состава рассматриваемых при моделировании видов политик управления доступом целесообразно осуществлять за счет возможности выражения политик одних видов политиками других видов.

Примечание - Традиционная для операционных систем политика дискреционного управления доступом при разработке формальной модели часто может быть выражена политикой ролевого управления доступом. При этом с используемыми в операционной системе учетными записями пользователей, группами учетных записей пользователей и с привилегиями могут быть сопоставлены одноименные роли.

4.5 Рекомендации по выбору технологий, инструментальных средств и практических приемов разработки формальной модели управления доступом приведены в разделе 5.

4.6 Рекомендации по описанию формальной модели, в том числе состояний и правил перехода между состояниями используемого для моделирования согласно ГОСТ Р 59453.1 абстрактного автомата, приведены в разделе 6.

4.7 Рекомендации по описанию и доказательству выполнения условий безопасности, в том числе при верификации формальной модели управления доступом, при демонстрации взаимосвязи этих условий безопасности с режимами функционирования средства защиты информации приведены в разделе 7.

5 Рекомендуемые технологии и практические приемы разработки формальной модели управления доступом

5.1 Для описания формальной модели управления доступом рекомендуется использовать математический и как минимум один из формализованных (машиночитаемых) языков. Это обусловлено тем, что применение математического описания формальной модели всегда допускает полную, независимую от разработчика, проверку корректности этого описания заданных в формальной модели условий безопасности, а также всех выполненных в модели доказательств (при этом согласно ГОСТ Р 59453.2 при верификации формальной модели для этого потребуется перевод ее математического описания в формализованное описание с представлением свидетельств их согласованности). Использование формализованного описания

позволяет с применением инструментальных средств, реализующих формальные методы, поддерживающие выбранный язык этого описания, осуществить автоматическую верификацию формальной модели, доказательство ее непротиворечивости.

Примечание - При описании формальной модели на математическом языке доказательство (используемые для этого логические рассуждения) ее непротиворечивости (в том числе выполнения условий безопасности) приводится непосредственно в этом описании, что предоставляет возможность объективного анализа корректности доказательства любым специалистом, знакомым с языком математики. При использовании формализованного языка (например, Alloy, B, Event-B, TLA+) автоматически с применением инструментальных средств, как правило, проще выявляются неточности описания формальной модели. Вместе с тем значительная часть логики автоматического доказательства непротиворечивости формальной модели реализуется непосредственно в инструментальных средствах, объективная проверка корректности результатов работы которых может быть затруднена.

5.2 При выборе инструментальных средств разработки формальной модели управления доступом целесообразно исходить из возможности их использования для автоматической верификации модели. В связи с этим инструментальные средства, используемые для автоматической верификации формальной модели управления доступом, должны удовлетворять критериям, установленным в ГОСТ Р 59453.2.

5.3 При разработке формальной модели управления доступом рекомендуется проанализировать существующие формальные модели, в первую очередь соответствующие рассматриваемым при моделировании видам реализуемых средством защиты информации политик управления доступом, а также среде функционирования средства (операционная система, система управления базами данных или другие). По результатам такого анализа целесообразно выбрать базовую формальную модель, на основе которой можно осуществлять дальнейшую разработку. Также в результате проведенного анализа кроме базовой формальной модели могут быть отобраны другие модели, элементы которых отсутствуют в базовой модели, если их целесообразно включить в разрабатываемую формальную модель как существенные для моделирования средства защиты информации. При этом следует отметить недостатки базовой формальной модели, не позволяющие ее использовать непосредственно для моделирования средства защиты информации (в том числе отсутствие в модели отражения существенных свойств средства защиты информации или среды его функционирования) и которые необходимо устранить в разрабатываемой формальной модели.

Примечание - Существенным для многих средств защиты информации, реализующих политики управления доступом, является использование иерархии объектов доступа (сущностей, например файлов и каталогов), привилегированных и непривилегированных учетных записей пользователей, привилегированных и непривилегированных субъектов доступа. Многие формальные модели, известные как классические (например, модели Bell-LaPadula, Take-Grant, RBAC), не моделируют перечисленные свойства средств защиты информации или среды их функционирования. Также эти модели не позволяют моделировать информационные потоки (скрытые каналы) по времени. Вместе с тем существуют формальные модели (например, семейства ДП-моделей), в которых эти свойства моделируются.

5.4 Для разработки формальной модели управления доступом целесообразно применять следующие технологии и практические приемы:

- поэтапное усложнение формальной модели, когда на каждом этапе, начиная с выбранной в

соответствии с 5.3 базовой формальной модели, свойства средства защиты информации или среды его функционирования моделируются по частям, при этом осуществляется описание текущего представления формальной модели, доказательство выполнения соответствующих этому представлению условий безопасности, а также верификация формальной модели.

Примечание - Формальная модель управления доступом может быть достаточно сложной, в связи с чем допущенные при ее описании возможные неточности или противоречия могут быть выявлены только на завершающем этапе ее разработки. При этом устранение этих неточностей или противоречий может потребовать полной переработки формальной модели. Использование поэтапного усложнения модели при ее разработке позволяет своевременно выявлять большинство неточностей или противоречий. Это осуществляется в первую очередь за счет доказательства выполнения условий безопасности, соответствующих каждому этапу разработки текущего представления формальной модели, а также верификации этого текущего представления формальной модели. Кроме того, каждый этап разработки формальной модели может соответствовать описанию в ее рамках только отдельного свойства (или нескольких свойств) средства защиты информации или среды его функционирования, что также упрощает моделирование;

- объединение нескольких формальных моделей управления доступом на основе выбранной в соответствии с 5.3 базовой формальной модели с учетом влияния свойств каждой из моделей на выполнение в результирующей формальной модели условий безопасности.

Примечание - Заимствование элементов нескольких формальных моделей управления доступом может оказаться необходимым для моделирования средства защиты информации, реализующего несколько политик управления доступом или состоящего из нескольких систем (например, операционная система и система управления базами данных), самостоятельно реализующих такие политики. При этом необходимо учитывать свойства каждой из моделей (соответствующих им политик управления доступом), в противном случае может оказаться невозможным доказательство выполнения в результирующей модели условий безопасности и, как следствие, соответствующие недостатки (уязвимости) могут быть присущи моделируемому средству защиты информации.

Пример - При моделировании мандатного управления доступом с применением элементов моделей ролевого управления доступом назначаемые ролям права доступа к объектам доступа могут быть использованы для создания нарушающих требования политики мандатного управления доступом информационных потоков (скрытых каналов) по времени от объектов доступа с бóльшим уровнем конфиденциальности к объектам доступа с меньшим уровнем конфиденциальности. Для предотвращения возможности возникновения таких скрытых каналов может быть использовано назначение ролям уровней конфиденциальности и предоставление их субъектам доступа в качестве текущих (в том числе возможности изменения ими прав доступа ролей) только в случае, когда уровень доступа соответствующего субъекта доступа не ниже уровня конфиденциальности соответствующей роли;

- разработка иерархического представления формальной модели управления доступом, состоящего из слоев (уровней), при этом каждый нижний слой этого представления формальной модели включает описание ее элементов, не зависящих от элементов, принадлежащих более высокому слою, который, в свою очередь, наследует, а при необходимости корректирует или дополняет элементы нижнего слоя.

Примечание - Использование иерархического представления формальной модели управления доступом существенно упрощает ее разработку, особенно в случае, когда моделируемое средство защиты информации реализует несколько политик управления доступом или оно состоит из нескольких систем (например, операционная система и система управления базами данных). Тогда с каждой политикой управления доступом или каждой системой может быть сопоставлен отдельный слой (или отдельные слои) иерархического представления формальной модели. При этом доказательство выполнения условий безопасности и верификация формальной модели могут быть осуществлены последовательно, по слоям. Выбор последовательности слоев при описании формальной модели в ее иерархическом представлении может быть осуществлен исходя из непосредственной технической реализации моделируемого средства защиты информации (например, слой, соответствующий операционной системе, будет ниже слоя, соответствующего системе управления базами данных);

- разработка на основе выбранной в соответствии с 5.3 базовой формальной модели управления доступом сокращенной (редуцированной) формальной модели, включающей подмножество элементов базовой формальной модели либо содержащей ограничения, обеспечивающие возможность применения инструментальных средств автоматической верификации модели.

Примечание - Разработка сокращенной (редуцированной) формальной модели управления доступом может потребоваться, когда базовая формальная модель включает некоторые элементы, избыточные для описания моделируемого средства защиты информации. Кроме того, это может потребоваться, когда из-за большей сложности затруднена верификация базовой формальной модели (например, из-за проблемы "комбинаторного взрыва" может стать невозможной верификация базовой формальной модели по методу проверки моделей - model checking). В том числе для применения инструментальных средств автоматической верификации по методу проверки моделей может быть ограничен состав элементов начального состояния, описываемого в рамках формальной модели абстрактного автомата;

- разработка отдельных формальных моделей для компонентов средства защиты информации с обоснованием отсутствия влияния каждого компонента на реализацию политик безопасности другими компонентами.

Примечание - В случае моделирования средства защиты информации, функционирующего в сетевой инфраструктуре и реализующего политики управления доступом, для которых, как правило, не существенны информационные потоки (например, политику дискреционного управления доступом), для компонентов такого средства (например, функционирующих на сервере или на рабочей станции) при наличии у них существенных отличий могут быть разработаны отдельные формальные модели управления доступом.

6 Рекомендации по описанию формальной модели управления доступом

6.1 Непосредственное описание формальной модели управления доступом рекомендуется начинать с состояний абстрактного автомата, которые должны включать элементы, перечисленные в ГОСТ Р 59453.1. При этом следует учитывать следующее:

- во множество учетных записей пользователей целесообразно включить не только элементы, которым соответствуют явно реализованные в моделируемом средстве защиты информации учетные записи пользователей, но также соответствующие учетным записям

системных пользователей (псевдопользователей). Если в моделируемом средстве отсутствуют явно реализованные учетные записи пользователей, рекомендуется включить в это множество либо не менее одного элемента для учетной записи системного пользователя (псевдопользователя), либо элементы для учетных записей, соответствующих наиболее близким по назначению компонентам средства защиты информации (например, при реализации в нем политики ролевого управления доступом для некоторых ролей могут быть заданы соответствующие им элементы множества учетных записей пользователей).

Примечание - Использование учетных записей, соответствующих системным пользователям (псевдопользователям, от имени которых, например, функционируют некоторые процессы ядра операционной системы), может позволить более точно смоделировать режимы функционирования средства защиты информации. Кроме того, при реализации в системах управления базами данных (например, в системе управления базами данных PostgreSQL) политики ролевого управления доступом учетные записи пользователей могут не задаваться вообще. Вместо них используются роли (называемые иногда ролями входа), с получения которых начинается сеанс работы в такой системе. С этими ролями при описании формальной модели могут быть сопоставлены одноименные элементы множества учетных записей пользователей;

- элементы множества субъектов доступа, как правило, ставятся в соответствие каждому субъекту доступа среды функционирования средства защиты информации.

Примечание - В некоторых случаях для упрощения описания формальной модели нескольким субъектам доступа может ставиться в соответствие один элемент множества субъектов доступа, например когда в одном сеансе от имени одной учетной записи пользователя функционируют обладающие одинаковыми правами доступа субъекты доступа (процессы);

- элементы множества объектов доступа, как правило, ставятся в соответствие каждому объекту доступа среды функционирования средства защиты информации. На этом множестве задается соответствующее используемому в моделируемом средстве защиты информации отношение иерархии.

Примечание - При моделировании средств защиты информации, таких как операционные системы или системы управления базами данных, которые могут включать миллионы объектов доступа, может потребоваться сокращение числа элементов множества объектов доступа. В случае системы управления базами данных такое моделирование может быть осуществлено, например, до таблиц базы данных. При этом права доступа и доступы субъектов доступа к записям таблиц могут быть смоделированы как права доступа и доступы к самим таблицам (например, доступ субъекта доступа на запись к записи таблицы может при моделировании описываться как доступ на запись к этой таблице целиком). Отношение иерархии на множестве объектов доступа описывается в соответствии с тем, как это отношение реализовано в моделируемом средстве защиты информации. Например, при моделировании операционных систем семейства Linux отношение иерархии должно позволять описывать "жесткие" ссылки (hard link), когда некоторый соответствующий файлу объект доступа (объект) может одновременно непосредственно подчиняться в иерархии нескольким объектам доступа, соответствующим каталогам (контейнерам);

- при описании множества реализуемых доступов субъектов к объектам доступа целесообразно учитывать, что для большинства моделируемых средств защиты информации и реализуемых ими политик управления доступом достаточно использовать только два вида

доступа: на чтение и на запись;

- при описании множества реализуемых прав доступа субъектов к объектам или субъектам доступа следует учитывать возможное многообразие способов задания таких прав в средствах защиты информации. Реализуемые права доступа могут быть как универсальными для всех субъектов или объектов доступа, так и зависящими от конкретного экземпляра субъекта или объекта доступа. Эти права доступа могут задаваться непосредственно или для этого могут использоваться группы, роли, типы, атрибуты или другие способы. При моделировании средства защиты информации, состоящего из нескольких систем (например, операционная система и система управления базами данных), самостоятельно реализующих политики управления доступом, рекомендуется задать отношение соответствия между правами доступа, используемыми в каждой из систем.

Примечание - Реализуемые в операционных системах права доступа субъектов доступа к объектам или субъектам доступа в большинстве случаев при моделировании можно рассматривать как универсальные (например, права доступа на чтение, запись, выполнение, владение). Вместе с тем в системах управления базами данных называемые привилегиями права доступа часто существенно зависят от назначения конкретных объектов доступа (например, в системах управления базами данных PostgreSQL к таблицам может назначаться широкий спектр привилегий: SELECT, INSERT, UPDATE, DELETE, TRUNCATE и другие, а к функциям - только привилегия EXECUTE), что необходимо учитывать при моделировании. Кроме того, в таких системах может потребоваться задание эффективных прав доступа (привилегий), когда, например, права доступа назначаются не непосредственно роли, а другой роли, у которой первая роль имеет право их наследовать (для этого может использоваться привилегия INHERIT), что также может существенно затруднить моделирование. К субъектам доступа, как правило, во множество реализуемых прав доступа достаточно включать только право доступа владения, которое, например, может соответствовать ситуации в операционных системах, когда к субъекту (процессу) другой субъект (процесс) имеет привилегию отладки. Задание отношения соответствия между правами доступа, реализуемыми в системах, из которых может состоять средство защиты информации, удобно для моделирования информационных потоков, возникающих между субъектами и объектами доступа этих систем (особенно при описании единых для моделируемого средства защиты информации правил перехода из состояний в состояния абстрактного автомата).

Пример - При моделировании средства защиты информации, состоящего из системы управления базами данных и операционной системы, отношение соответствия между некоторыми правами доступа (привилегиями), используемыми в первой системе, и правами доступа, используемыми во второй системе, может быть задано следующим образом:

SELECT (привилегия получать строки из таблицы) - $read_r$ (право доступа на чтение);

INSERT (привилегия добавлять строки в таблицу) - $write_r$ (право доступа на запись);

EXECUTE (привилегия выполнить функцию) - $execute_r$ (право доступа на выполнение);

UPDATE (привилегия изменять строки в таблице) - $read_r$ (право доступа на чтение), $write_r$ (право доступа на запись);

- при описании множества информационных потоков целесообразно включить в него информационные потоки по памяти. Включение в него информационных потоков по времени

рекомендуется при моделировании средства защиты информации, реализующего политику мандатного управления доступом.

Примечание - В средствах защиты информации, реализующих мандатное управление доступом, нарушением условий безопасности является создание информационного потока (скрытого канала) от объекта доступа к другому объекту доступа, первый из которых обладает несравнимым или более высоким уровнем конфиденциальности, чем у второго объекта доступа. Таким информационным потоком может быть поток по времени. При этом для средств защиты информации, реализующих политики дискреционного, ролевого управления доступом или мандатного контроля целостности, информационные потоки по времени, как правило, не могут быть использованы для нарушения условий безопасности, поэтому их нецелесообразно описывать при моделировании таких средств;

- при разработке формальной модели управления доступом условия внутренней и взаимной корректности (согласованности) используемых для описания состояний абстрактного автомата множеств, функций (отношений) целесообразно явно формулировать, основываясь на логике применения этих функций и отношений, исходя из необходимости обеспечения их соответствия компонентам, свойствам моделируемого средства защиты информации и реализуемых им политик управления доступом. Для сокращения числа неточностей или противоречий, допущенных при разработке формальной модели, проверку выполнения этих условий рекомендуется осуществлять сразу при появлении такой возможности, в том числе после каждого этапа разработки формальной модели (если в соответствии с 5.4 выполняется поэтапное усложнение формальной модели) или после описания каждого слоя представления формальной модели (если в соответствии с 5.4 разрабатывается иерархическое представление формальной модели). Кроме того, эти условия рекомендуется использовать при формализованном описании и автоматической верификации формальной модели.

Пример - Условия внутренней и взаимной корректности (согласованности) множеств, функций (отношений), используемых для описания состояний абстрактного автомата:

- в иерархии объектов доступа (сущностей) только являющиеся объектами доступа контейнеры могут содержать другие объекты доступа;

- субъекты доступа могут иметь друг к другу только право доступа владения;

- если учетной записи пользователя разрешена некоторая роль, то этой учетной записи пользователя разрешены все роли, подчиненные первой роли (изначально разрешенной) в иерархии ролей;

- в иерархии объектов доступа (сущностей) объекты доступа, находящиеся выше в иерархии, имеют уровень целостности не ниже уровней целостности объектов доступа, находящихся ниже в иерархии;

- уровень доступа субъекта доступа не превосходит уровня доступа учетной записи пользователя, от имени которой он функционирует.

6.2 В рамках формальной модели управления доступом рекомендуется описать правила перехода из состояний в состояния абстрактного автомата (параметры каждого правила, условия и результаты его применения), позволяющие модифицировать (создавать, удалять, изменять значение или параметры) элементы этих состояний, за исключением случаев, когда

соответствующие изменения не предусмотрены режимами функционирования моделируемого средства защиты информации. При этом желательно, чтобы с каждой непосредственно связанной с реализацией политик управления доступом функцией (системным вызовом, хранимой процедурой, событием или другое) средства защиты информации было сопоставлено правило(а) перехода из состояний в состояния абстрактного автомата (при этом допускается, чтобы одному правилу соответствовало несколько функций). Эти правила рекомендуется включить в первую группу правил (де-юре правил). Во вторую группу правил (де-факто правил) рекомендуется включить правила, не соответствующие каким-либо функциям средства защиты информации, а используемые для описания и доказательства выполнения условий безопасности. В том числе во вторую группу правил могут быть включены правила, предназначенные для создания информационных потоков или получения за счет использования этих информационных потоков субъектами доступа управления другими субъектами доступа. Также для каждого правила в его параметрах, условиях и результатах применения следует указывать субъекта(ов) доступа, который может являться инициатором выполнения этого правила.

Примечание - Существуют средства защиты информации (например, встраиваемые операционные системы), в которых явно могут не реализовываться учетные записи пользователей. При моделировании таких средств не имеет смысла описывать правила перехода из состояний в состояния абстрактного автомата, позволяющие администрировать учетные записи пользователей (создавать, изменять их параметры, удалять). Порядок сопоставления функций средства защиты информации и правил перехода из состояний в состояния абстрактного автомата зависит от свойств этого средства, удобства при моделировании и применяемых для этого технологий (например, с системным вызовом в операционных системах, осуществляющим создание или открытие файла, может быть сопоставлено два правила: для создания объекта доступа и для получения доступа к объекту доступа; наоборот, одно правило создания объекта доступа может описывать несколько системных вызовов для создания файлов, каталогов, сокетов или других сущностей). Если состав и описание де-юре правил, как правило, сильно зависят от моделируемого средства защиты информации, то состав и описание де-факто правил достаточно универсальны (в качестве их примера при разработке формальной модели удобно использовать де-факто правила из расширенной модели Take-Grant или семейства ДП-моделей). Явное задание в каждом де-юре и де-факто правиле перехода из состояний в состояния абстрактного автомата субъекта(ов) доступа, как инициатора его выполнения, соответствует тому, что только субъекты доступа (например, процессы), как активные компоненты среды функционирования средства защиты информации, могут инициировать выполнение каких-либо функций этого средства.

6.3 При описании в соответствии с 6.1 и 6.2 состояний и правил перехода из состояний в состояния абстрактного автомата следует учитывать перспективы дальнейшего формулирования условий безопасности, математического или формального (при верификации формальной модели управления доступом с применением инструментальных средств) доказательства их выполнения согласно рекомендациям, изложенным в разделе 7. Для этого при наличии возможности правила перехода из состояний в состояния абстрактного автомата, в которые только добавляются новые элементы состояний, следует описывать отдельно от правил, в которых эти элементы удаляются. В условиях и результатах применения правил первой группы (де-юре правил), описанных согласно 6.2, целесообразно избегать использования информационных потоков или управления одними субъектами доступа другими субъектами доступа. Наоборот, в результатах применения правил второй группы (де-факто правил) не следует вносить изменения в элементы описания состояний абстрактного автомата, которые непосредственно реализуются в средстве защиты информации. Если в соответствии с 5.4 разрабатывается иерархическое представление формальной модели, то используемые при описании условий и результатов применения правил

элементы состояний рекомендуется также распределять по слоям, которым эти элементы соответствуют. Также рекомендуется определить ограничения и особенности формальных методов и реализующих их инструментальных средств, которые необходимо учесть при разработке формальной модели управления доступом и которые могут повлиять на успешность использования этих средств для верификации формальной модели. Для учета этих ограничений целесообразно использовать разработку согласно 5.4 сокращенной (редуцированной) формальной модели (в том числе путем уменьшения числа элементов описания состояний абстрактного автомата, особенно его начального состояния) или отдельных формальных моделей для каждого компонента средства защиты информации.

Примечание - Возможность описать правила перехода из состояний в состояния абстрактного автомата (монотонные правила), в которые только добавляются новые элементы состояний, отдельно от правил (немонотонных правил), в которых эти элементы удаляются, иногда упрощает математическое доказательство выполнения условий безопасности (особенно в случае, когда моделируемое средство защиты информации реализует дискреционное управление доступом). Большинство инструментальных средств автоматической верификации по методу проверки моделей (model checking) чувствительны к числу элементов состояний описываемого в рамках формальной модели абстрактного автомата. Учесть такое ограничение часто можно за счет разработки сокращенной (редуцированной) формальной модели или (при наличии такой возможности) отдельных формальных моделей для каждого компонента средства защиты информации.

6.4 Если моделируемое средство защиты информации реализует политику дискреционного управления доступом, то при разработке формальной модели управления доступом дополнительно рекомендуется выбрать способ описания матрицы доступов, наиболее соответствующий тому, как она непосредственно задается в этом средстве.

Примечание - В большинстве средств защиты информации, реализующих политику дискреционного управления доступом, матрица доступов задается назначением каждому объекту доступа права доступа к нему субъектов доступа либо с помощью маски бит (например, как в операционных системах семейства Linux), либо с помощью списков контроля доступа (например, как в операционных системах семейства Windows). Применение способов описания матрицы доступов, не связанных с тем, как она задается в средстве защиты информации, может, с одной стороны, обеспечить большую наглядность и удобство при моделировании (например, при использовании для этого графа прав доступа, как в модели Take-Grant), с другой стороны, это может затруднить демонстрацию взаимосвязи описанных в формальной модели условий безопасности с режимами функционирования этого средства.

6.5 Если моделируемое средство защиты информации реализует политику ролевого управления доступом, то при разработке формальной модели управления доступом дополнительно рекомендуется:

- во множестве ролей задать подмножество административных ролей, позволяющих обладающим ими в качестве текущих субъектов доступа администрировать ролевое управление доступом (создавать или удалять роли, изменять их иерархию, задавать права доступа ролей, изменять множества ролей, разрешенных для учетных записей пользователей, и осуществлять другие действия с ролями).

Примечание - Если в моделируемом средстве защиты информации имеются административные роли, которые либо не могут непосредственно создавать, удалять, изменять в

процессе функционирования этого средства свои параметры (например, роль postgres в системе управления базами данных PostgreSQL), либо такое предположение допустимо при моделировании, то для упрощения описания формальной модели управления доступом (особенно правил перехода из состояний в состояния абстрактного автомата) во множестве ролей рекомендуется задать подмножество соответствующих (часто называемых системными) административных ролей;

- для упрощения описания формальной модели целесообразно избегать включения в него несущественных для реализации политики ролевого управления доступом параметров ролей (например, имена ролей), за исключением случаев, когда эти параметры необходимы для моделирования других реализуемых средством защиты информации политик управления доступом.

Примечание - Имена ролей в большинстве случаев несущественны при разработке формальной модели средства защиты информации, реализующего политику ролевого управления доступом. В то же время если такое средство также реализует политику мандатного управления доступом, то имена ролей могут использоваться для создания информационных потоков (скрытых каналов) по времени. В таком случае имена ролей целесообразно включать в описание разрабатываемой формальной модели;

- если средство защиты информации состоит из нескольких систем, самостоятельно реализующих политику ролевого управления доступом, то объединение при моделировании используемых в этих системах ролей в единое множество, задание общих для всех ролей параметров следует осуществлять исходя из удобства моделирования, упрощения описания формальной модели, а также обеспечения возможности демонстрации взаимосвязи описанных в ней условий безопасности с режимами функционирования моделируемого средства.

6.6 Если моделируемое средство защиты информации реализует политику мандатного контроля целостности, то при разработке формальной модели управления доступом дополнительно рекомендуется:

- учесть при задании множеств учетных записей привилегированных и непривилегированных пользователей важность корректного включения в соответствующее множество каждой конкретной учетной записи пользователя исходя из наличия или отсутствия у него полномочий по управлению или администрированию моделируемого средства защиты информации.

Примечание - Избыточное включение учетных записей пользователей во множество непривилегированных учетных записей пользователей может привести к невозможности математического (формального) доказательства того, что в абстрактном автомате выполняются условия безопасности (функционирующие от имени таких непривилегированных учетных записей пользователей непривилегированные субъекты доступа будут иметь, например, права доступа или привилегии, соответствующие привилегированным учетным записям пользователей). Наоборот, необоснованное включение учетных записей пользователей во множество привилегированных учетных записей пользователей может позволить доказать выполнение этих условий безопасности, хотя это не будет соответствовать режимам функционирования моделируемого средства защиты информации;

- задать привилегированным учетным записям пользователей и привилегированным субъектам доступа максимальный в решетке уровней целостности уровень целостности, а

непривилегированным учетным записям пользователей и непривилегированным субъектам доступа - уровни целостности меньше максимального в решетке уровней целостности уровня целостности (в том числе минимальный в решетке уровней целостности уровень целостности);

- включить в описание разрабатываемой формальной модели управления доступом множество информационных потоков по памяти, а также предназначенные для использования таких информационных потоков и описанные в 6.2 правила перехода из состояний в состояния абстрактного автомата второй группы (де-факто правила), поскольку информационные потоки по памяти существенны для описания условий безопасности при моделировании средств защиты информации, реализующих политику мандатного контроля целостности;

- задать для каждого субъекта доступа множество функционально ассоциированных с ним объектов доступа, что является существенным для описания условий безопасности, связанных с наличием возможности у одних субъектов доступа (особенно непривилегированных) получать управление другими субъектами доступа (особенно привилегированными).

Примечание - В большинстве средств защиты информации (например, в операционных системах) у каждого субъекта доступа есть хотя бы один функционально ассоциированный с ним объект доступа. Например, для каждого процесса операционной системы (субъекта доступа) существует исполняемый файл (объект доступа), из которого этот процесс был инициализирован. При этом такими объектами доступа могут быть также файлы динамических библиотек, конфигурационные файлы, сегменты оперативной памяти, записи, содержащие функции или триггеры систем управления базами данных, и другие;

- задать (при необходимости) подмножество привилегированных субъектов доступа, доступы которых к объектам доступа не могут быть использованы для создания информационных потоков по памяти от непривилегированных субъектов доступа к объектам доступа, функционально ассоциированным с привилегированными субъектами доступа.

Примечание - В большинстве средств защиты информации существуют объекты доступа (например, сокеты в операционных системах), через которые могут осуществлять обмен данными привилегированные и непривилегированные субъекты доступа. При этом такие объекты доступа часто имеют минимальный в решетке уровней целостности уровень целостности. В результате к ним могут получать доступы на запись непривилегированные субъекты доступа, а на чтение - привилегированные субъекты доступа, которые, в свою очередь, могут получать доступ на запись к объектам доступа, функционально ассоциированным с другими привилегированными субъектами доступа. Если непосредственно описать это в разрабатываемой формальной модели управления доступом, то возможна ситуация, когда с участием привилегированных субъектов доступа возможно создание информационных потоков по памяти от непривилегированных субъектов доступа к объектам доступа, функционально ассоциированным с привилегированными субъектами доступа, что будет приводить к нарушению условий безопасности (например, к получению управления непривилегированными субъектами доступа привилегированными субъектами доступа). Для предотвращения этого в средствах защиты информации доступы на чтение привилегированных субъектов доступа к объектам доступа, через которые ими осуществляется обмен данными с непривилегированными субъектами доступа, реализуется таким образом, чтобы эти доступы (например, через интерфейсы сокетов операционных систем) не могли использоваться для создания информационных потоков по памяти, приводящих к нарушению условий безопасности. Это целесообразно учесть при разработке формальной модели управления доступом путем задания соответствующего подмножества привилегированных субъектов доступа (часто называемого

корректным);

- при разработке формальной модели, если средство защиты информации состоит из нескольких систем, самостоятельно реализующих политику мандатного контроля целостности, задать единые для всех этих систем решетку уровней целостности, функции (отношения), используемые для задания уровней целостности учетных записей пользователей, субъектов и объектов доступа, а также множество информационных потоков по памяти.

Примечание - В средстве защиты информации, состоящем из нескольких систем (например, операционной системы и системы управления базами данных), доступы субъектов доступа к объектам доступа одной системы могут быть использованы для нарушения условий безопасности при реализации политики мандатного контроля целостности в другой системе. Например, доступы процессов (субъектов доступа) к файлам операционной системы (объектам доступа), в которых содержатся записи (объекты доступа) системы управления базами данных. Аналогично для этого могут использоваться информационные потоки по памяти между субъектами и объектами доступа этих систем. Поэтому при моделировании таких средств рекомендуется задание единых для всех систем решетки уровней целостности, функций (отношений), используемых для задания уровней целостности учетных записей пользователей, субъектов и объектов доступа, множества информационных потоков по памяти. При наличии такой возможности целесообразно также задание единых правил перехода из состояний в состояния абстрактного автомата;

- использовать решетку уровней целостности, содержащую меньшее число элементов, чем реализовано в моделируемом средстве защиты информации, для упрощения описания формальной модели управления доступом, в том числе когда согласно 5.4 разрабатывается сокращенная (редуцированная) формальная модель.

Примечание - Для описания большинства условий безопасности при моделировании средств защиты информации, реализующих политику мандатного контроля целостности, могут оказаться достаточными всего два уровня целостности, например "высокая целостность" (для привилегированных учетных записей пользователей, функционирующих от их имени субъектов доступа, функционально ассоциированных с ними объектов доступа) и "низкая целостность" (для остальных учетных записей пользователей, субъектов и объектов доступа). Кроме того, использование решетки уровней целостности, состоящей из меньшего числа элементов, чем в моделируемом средстве защиты информации, может быть полезным при верификации формальной модели по методу проверки моделей (model checking), так как инструментальные средства, реализующие этот метод, чувствительны к числу элементов состояний описываемого абстрактного автомата.

6.7 Если моделируемое средство защиты информации реализует политику мандатного управления доступом, то при разработке формальной модели управления доступом дополнительно рекомендуется:

- включить в описание разрабатываемой формальной модели управления доступом множество(а) информационных потоков по памяти и по времени, а также предназначенные для использования таких информационных потоков и описанные в 6.2 правила перехода из состояний в состояния абстрактного автомата второй группы (де-факто правила), поскольку информационные потоки по памяти и по времени существенны для описания условий безопасности при моделировании средств защиты информации, реализующих политику мандатного управления доступом;

- использовать при разработке формальной модели управления доступом в соответствии с 5.4 ее иерархическое представление, состоящее как минимум из двух слоев, на первом из которых при описании формальной модели использовать только множество информационных потоков по памяти, на втором слое - множество информационных потоков по памяти и по времени.

Примечание - В отличие от информационных потоков по памяти при разработке формальной модели управления доступом описание информационных потоков по времени, а также предназначенных для их использования правил перехода из состояний в состояния абстрактного автомата, как правило, является более сложной задачей. Поэтому для упрощения разработки формальной модели, сокращения допущенных при ее описании неточностей или противоречий целесообразно использование ее иерархического представления, где на первом слое описывается только множество информационных потоков по памяти, а на втором слое - множество информационных потоков по памяти и по времени;

- при разработке формальной модели средства защиты информации, состоящего из нескольких систем, самостоятельно реализующих политику мандатного управления доступом, задать единые для всех этих систем решетку уровней конфиденциальности, функции (отношения), используемые для задания уровней доступа учетных записей пользователей и субъектов доступа, уровней конфиденциальности объектов доступа, а также множество информационных потоков по памяти и по времени.

Примечание - В средстве защиты информации, состоящем из нескольких систем (например, операционной системы и системы управления базами данных), доступы субъектов доступа к объектам доступа одной системы могут быть использованы для нарушения условий безопасности при реализации политики мандатного управления доступом в другой системе (аналогично средствам защиты информации, в которых реализуется политика мандатного контроля целостности). Особенно такие доступы могут быть использованы для создания запрещенных этими условиями безопасности информационных потоков по времени между объектами доступа (например, от объектов доступа с бóльшим уровнем конфиденциальности к объектам доступа с меньшим уровнем конфиденциальности) систем, из которых состоит средство защиты информации. Поэтому при моделировании таких средств рекомендуется задание единых для всех систем решетки уровней конфиденциальности, функций (отношений), используемых для задания уровней доступа учетных записей пользователей и субъектов доступа, уровней конфиденциальности объектов доступа, множества информационных потоков по памяти и по времени. При наличии такой возможности целесообразно также задание единых правил перехода из состояний в состояния абстрактного автомата;

- использовать решетку уровней конфиденциальности, содержащую меньшее число элементов, чем реализовано в моделируемом средстве защиты информации, для упрощения описания формальной модели управления доступом, в том числе когда согласно 5.4 разрабатывается сокращенная (редуцированная) формальная модель.

Примечание - Для описания большинства условий безопасности при моделировании средств защиты информации, реализующих политику мандатного управления доступом (аналогично политике мандатного контроля целостности), может оказаться достаточно всего двух уровней конфиденциальности (например, "высокая конфиденциальность" и "низкая конфиденциальность"). Это также может быть полезным при верификации формальной модели управления доступом по методу проверки моделей (model checking), так как инструментальные

средства, реализующие этот метод, чувствительны к числу элементов состояний описываемого абстрактного автомата.

7 Рекомендации по описанию и доказательству выполнения условий безопасности

7.1 Согласно ГОСТ Р 59453.1 при разработке формальной модели управления доступом должны быть описаны условия безопасности состояний абстрактного автомата и условия безопасности переходов из состояний в состояния абстрактного автомата. Для этого рекомендуется использовать определения политик управления доступом, которые следует с применением описанных в 5.4 технологий и практических приемов (поэтапное усложнение формальной модели, объединение нескольких формальных моделей, разработка иерархического представления формальной модели, сокращенной формальной модели или отдельных формальных моделей) конкретизировать с учетом деталей реализации этих политик в моделируемом средстве защиты информации. При этом следует формулировать условия безопасности так, чтобы проверка их выполнения являлась алгоритмически разрешимой задачей (для чего может потребоваться явно задавать необходимые допущения или исключения из этих условий).

Примечание - Существуют формальные модели управления доступом, в которых заданы условия безопасности, проверка выполнения которых является алгоритмически неразрешимой задачей (например, предназначенная для моделирования средств защиты информации, реализующих политику дискреционного управления доступом, модель Harrison-Ruzzo-Ullman) или алгоритмически разрешимой задачей (например, предназначенная для моделирования средств защиты информации, реализующих политику мандатного управления доступом, модель Bell-LaPadula).

Пример - Согласно определению политики мандатного управления доступом при получении доступа на чтение к объекту доступа уровень доступа субъекта доступа должен быть не ниже уровня конфиденциальности объекта доступа, а на запись - уровень доступа субъекта доступа должен быть не выше уровня конфиденциальности объекта доступа. Вместе с тем в операционных системах семейства Linux существуют объекты доступа (например, файлы /dev/null и /dev/zero), доступ на чтение и запись к которым необходимо разрешить субъектам доступа с любым уровнем доступа. Для учета этого при описании условий безопасности целесообразно для таких объектов доступа сделать соответствующее исключение.

7.2 Кроме условий безопасности состояний абстрактного автомата целесообразно определить дополнительные условия безопасности его начального состояния (или начальных состояний).

Примечание - При описании дополнительных условий безопасности начального состояния абстрактного автомата рекомендуется стремиться к упрощению математического (формального) доказательства выполнения всех условий безопасности (состояний абстрактного автомата и безопасности переходов из состояний в состояния абстрактного автомата). При этом важно учитывать режимы функционирования моделируемого средства защиты информации (например, такими дополнительными условиями могут быть требования к отсутствию в начальном состоянии информационных потоков или доступов субъектов доступа к объектам доступа).

7.3 При описании условий безопасности переходов из состояний в состояния абстрактного

автомата, исходя из режимов функционирования моделируемого средства защиты информации и реализуемых им политик управления доступом, рекомендуется накладывать ограничения на состав и параметры используемых при этом правил перехода между состояниями абстрактного автомата.

Пример - При моделировании средства защиты информации, реализующего политику мандатного контроля целостности, может быть задано ограничение, что инициаторами выполнения правил перехода между состояниями абстрактного автомата (соответствующими параметрами этих правил) могут быть только непривилегированные субъекты доступа. Такое ограничение может соответствовать режиму функционирования средства защиты информации, когда привилегированные субъекты доступа выполнили свои функции по его администрированию и в нем функционируют только непривилегированные субъекты доступа.

7.4 Если моделируемое средство защиты информации реализует политику дискреционного управления доступом, то при описании условий безопасности дополнительно рекомендуется описать условия, в которых накладываются ограничения на предоставление субъектам доступа (учетным записям пользователей, от имени которых они функционируют), которые не должны осуществлять управление или администрирование моделируемым средством защиты информации, прав доступа к субъектам или объектам доступа, позволяющих выполнять такие функции.

7.5 Если моделируемое средство защиты информации реализует политику ролевого управления доступом, то при описании условий безопасности дополнительно рекомендуется описать условия, в которых накладываются следующие ограничения:

- на предоставление ролям, которыми как текущими могут обладать субъекты доступа, не осуществляющие управление или администрирование моделируемым средством защиты информации, прав доступа (привилегий) к субъектам или объектам доступа, позволяющих выполнять такие функции;

- на обладание субъектами доступа, не осуществляющими управление или администрирование моделируемым средством защиты информации, административными ролями, если подмножество таких ролей задано в соответствии с 6.5.

7.6 Если моделируемое средство защиты информации реализует политику мандатного контроля целостности, то при описании условий безопасности дополнительно рекомендуется задать следующие ограничения:

- на уровень целостности каждого субъекта доступа, который должен быть не выше уровня целостности учетной записи пользователя, от имени которой он функционирует;

- на уровень целостности каждого объекта доступа, который должен быть не выше уровня целостности объекта доступа (контейнера), в составе которого находится первый объект доступа;

- на уровень целостности каждого объекта доступа, функционально ассоциированного с субъектом доступа, который должен быть не ниже уровня целостности этого субъекта доступа;

- на возможность управления субъектом доступа другим субъектом доступа, только в случае, когда уровень целостности первого субъекта доступа не ниже уровня целостности

второго субъекта доступа;

- на информационные потоки по памяти, из которых должны быть запрещены такие информационные потоки от любого субъекта доступа к объекту доступа, функционально ассоциированному с каким-либо субъектом доступа, когда уровень целостности первого субъекта доступа меньше или не сравним с уровнем целостности этого объекта доступа.

7.7 Если моделируемое средство защиты информации реализует политику мандатного управления доступом, то при описании условий безопасности дополнительно рекомендуется задать следующие ограничения:

- на уровень доступа каждого субъекта доступа, который должен быть не выше уровня доступа учетной записи пользователя, от имени которой он функционирует;

- на уровень конфиденциальности каждого объекта доступа, который должен быть не выше уровня конфиденциальности объекта доступа (контейнера), в составе которого находится первый объект доступа;

- на уровень конфиденциальности каждого объекта доступа, функционально ассоциированного с субъектом доступа, который либо должен быть равен уровню доступа этого субъекта доступа, либо если в моделируемом средстве защиты информации реализуется политика мандатного контроля целостности, то уровень целостности этого объекта доступа равен максимальному в решетке уровней целостности уровню целостности;

- на возможность управления субъектом доступа другим субъектом доступа, только в случае, когда уровень доступа первого субъекта доступа равен уровню доступа второго субъекта доступа;

- на информационные потоки по памяти и по времени, из которых должны быть запрещены такие информационные потоки от любого объекта доступа к другому объекту доступа, когда уровень конфиденциальности первого объекта доступа не сравним или выше уровня конфиденциальности второго объекта доступа.

7.8 Для демонстрации взаимосвязи условий безопасности с режимами функционирования моделируемого средства защиты информации рекомендуется путем задания соответствующих ему конкретных значений элементов описания состояний абстрактного автомата (множествам учетных записей пользователей, субъектов доступа, объектов доступа, прав доступа, доступов и другим, используемым для этого функциям, отношениям) осуществлять проверку соответствия выполнения этих условий безопасности при применении правил перехода между состояниями абстрактного автомата (начиная с его начального состояния) изменениям в части параметров, настроек средства защиты информации, используемых для реализации им политик управления доступом. Если используемые для верификации формальной модели управления доступом инструментальные средства позволяют задавать значения элементов описания состояний абстрактного автомата и изменения этих значений при применении правил перехода между его состояниями (описывать траектории его функционирования), то рекомендуется проверять соответствие этих переходов между состояниями абстрактного автомата изменениям параметров, настроек средства защиты информации, происходящим в результате соответствующих таким правилам действий над ним (например, вызовам системных интерфейсов в операционных системах или запросам, вызовам функций или триггеров в системах управления базами данных).

Примечание - При верификации формальной модели управления доступом по методу проверки моделей (model checking), как правило, реализующие его инструментальные средства позволяют задавать траектории состояний абстрактного автомата. В таком случае для демонстрации взаимосвязи условий безопасности с режимами функционирования средства защиты информации удобно проверять соответствие этих траекторий результатам выполнения последовательностей моделируемых правилами переходов между состояниями абстрактного автомата действий в средстве защиты информации.

7.9 При доказательстве выполнения условий безопасности в случае, когда для описания формальной модели управления доступом используется математический язык, рекомендуется осуществлять его (как правило, вручную) с использованием метода математической индукции по длине последовательности состояний абстрактного автомата, сделав предположение от противного - о невыполнении условий безопасности в конечном состоянии такой последовательности - и приходя в связи с этим к противоречию.

7.10 При доказательстве выполнения условий безопасности в случае, когда для описания формальной модели управления доступом используется формализованный (машиночитаемый) язык, следует руководствоваться рекомендациями ГОСТ Р 59453.2, осуществляя доказательство автоматически, а при невозможности такого доказательства - выполняя интерактивное доказательство.

Примечание - При доказательстве выполнения условий безопасности с применением инструментальных средств целесообразно использовать различные технологии верификации формальной модели управления доступом (например, дедуктивную верификацию и верификацию по методу проверки моделей - model checking). Это позволяет своевременно выявлять большее число ошибок или дефектов, допущенных при описании формальной модели.

7.11 Если при разработке формальной модели в соответствии с 5.4 применяются технологии и практические приемы поэтапного усложнения описания формальной модели, разработки иерархического представления формальной модели или отдельных формальных моделей, то рекомендуется осуществлять доказательство выполнения условий безопасности, соответственно, после окончания каждого этапа описания формальной модели, разработки каждого слоя ее иерархического представления или каждой отдельной формальной модели (для каждого из компонентов, из которых в этом случае состоит моделируемое средство защиты информации).

7.12 В случае, когда в соответствии с 5.4 для каждого из компонентов моделируемого средства защиты информации разрабатываются отдельные формальные модели управления доступом, рекомендуется (при наличии такой возможности) осуществить доказательство отсутствия влияния каждого из компонентов на выполнение условий безопасности в других компонентах.

УДК 004.056:006.354 ОКС 35.030

Ключевые слова: защита информации, формальная модель управления доступом, средство защиты информации, политика управления доступом, политика дискреционного управления доступом, политика мандатного контроля целостности, политика мандатного управления доступом, политика ролевого управления доступом, верификация формальной модели управления доступом