ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59453.2— 2021

Защита информации

ФОРМАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

Часть 2

Рекомендации по верификации формальной модели управления доступом

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Обществом с ограниченной ответственностью «РусБИТех-Астра» (ООО «РусБИТех-Астра»), Институтом системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН)

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 22 апреля 2021 г. № 271-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 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.gost.ru)

Содержание

Введение

Верификация формальных моделей управления доступом используется для обеспечения доверия к средствам защиты информации, реализующим политики управления доступом, и уменьшает число недостатков при проектировании этих средств.

Применение инструментальных средств верификации формальных моделей управления доступом, реализуемых этими средствами формальных методов и поддерживаемых языков, технологий их использования и оценки полученных ими результатов верификации позволяет повысить уверенность в корректности этих формальных моделей.

В связи с этим настоящий стандарт устанавливает рекомендации по верификации формальных моделей управления доступом с применением инструментальных средств.

Настоящий стандарт применяется совместно с ГОСТ Р 59453.1—2021 «Защита информации. Формальная модель управления доступом. Часть 1. Общие положения».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ФОРМАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

Часть 2

Рекомендации по верификации формальной модели управления доступом

Information protection. Formal access control model. Part 2.
Recommendations on verification of formal access control model

Дата введения — 2021—06—01

1 Область применения

Настоящий стандарт представляет собой рекомендации по верификации с применением инструментальных средств 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 применена нормативная ссылка на следующий стандарт:

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

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 термины по ГОСТ Р 59453.1, а также следующие термины с соответствующими определениями:

Издание официальное

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

3.2 **инструментальное средство верификации:** Инструментальное средство, реализующее формальные методы верификации формальных моделей.

Примечание — Инструментальное средство верификации, как правило, поддерживает и формальные методы разработки формальных моделей.

3.3 **формализованное (машиночитаемое) описание:** Описание формальной модели на формальном языке со строгой и однозначно определенной семантикой, позволяющее использовать инструментальные средства верификации.

3.4 **формальный метод:** Основанный на математике и логике метод, а также поддерживаемые им языки, для верификации или разработки формальных моделей.

4 Общие положения

4.1 Для верификации формальной модели управления доступом, описание которой соответствует критериям, установленным ГОСТ Р 59453.1, должен быть осуществлен выбор соответствующих инструментальных средств, для которых должны быть представлены свидетельства, что реализуемые ими формальные методы позволяют осуществить верификацию формальной модели. При этом выбранные инструментальные средства должны допускать полную, независимую от их разработчиков проверку корректности результатов их работы.

4.2 Для верификации с использованием инструментальных средств формальная модель должна иметь формализованное (машиночитаемое) описание на языке, поддерживаемом реализуемыми этими инструментальными средствами формальными методами. Если формальная модель имеет математическое описание, то оно должно быть переведено в формализованное (машиночитаемое) описание на этом языке. При этом должны быть представлены свидетельства согласованности математического и формализованного (машиночитаемого) описаний формальной модели.

Примечание — Для формализованного (машиночитаемого) описания формальной модели управления доступом, как правило, используются формальные методы (Alloy, ASM, B, Event-B, TLA+, VDM-SL, Z), языки которых позволяют строить абстрактные автоматные модели. Примерами инструментальных средств, реализующих эти формальные методы, являются Rodin, TLA Toolbox. Кроме моделирования на основе абстрактных автоматных моделей, для верификации формальных моделей управления доступом могут использоваться темпоральные логики, сети Петри и другие формальные методы.

4.3 Верификация формальной модели управления доступом должна быть осуществлена путем применения к ее формализованному (машиночитаемому) описанию инструментальных средств верификации.

4.4 Верификация формальной модели управления доступом является успешной, если результаты применения инструментальных средств верификации к ее формализованному (машиночитаемому) описанию позволяют сделать вывод о непротиворечивости формальной модели и о выполнении заданных в ее рамках условий безопасности.

5 Выбор инструментальных средств верификации формальной модели управления доступом

5.1 При верификации формальной модели управления доступом должны быть разработаны критерии выбора инструментальных средств верификации, соответствие которым позволяет сделать вывод о том, что реализуемые этими инструментальными средствами формальные методы дают возможность осуществить верификацию формальной модели управления доступом.

5.2 Критерии выбора языка формализованного (машиночитаемого) описания формальной модели управления доступом должны быть основаны на оценке его возможностей (наличие теоретико-множественных примитивов и средств описания сложных структур данных) для представления описываемых в рамках формальной модели состояний и правил перехода из состояний в состояния абстрактного автомата.

5.3 Критерии выбора инструментальных средств верификации, реализующих формальные методы, поддерживающие соответствующий сформированным согласно 5.2 критериям язык формализован-

ного (машиночитаемого) описания формальной модели управления доступом, должны быть основаны на оценке характеристик этих инструментальных средств, включая:

- функциональные характеристики: возможность полной, независимой от разработчиков инструментальных средств верификации проверки корректности результатов их работы; возможность автоматического и интерактивного доказательства, автоматической или полуавтоматической генерации условий верификации (инвариантов), повторного использования ранее полученных доказательств выполнения условий верификации (переиспользования артефактов), создаваемых в ходе верификации; ограничения на размер абстрактного автомата; скорость верификации;

- нефункциональные характеристики: наличие реализуемой инструментальными средствами среды редактирования и верификации формализованного (машиночитаемого) описания формальной модели, анализа ошибок формальной модели; возможности по подключению и комбинированного использования библиотек (пруверов — инструментов для доказательства теорем, солверов — инструментов для решения систем уравнений); наличие успешного опыта применения разработчиками средств защиты информации, органами по сертификации и испытательными лабораториями; требования к среде эксплуатации, операционной системе, ресурсам оперативной и внешней памяти; стоимость; вид лицензии; наличие учебных материалов.

5.4 Должны быть представлены свидетельства соответствия выбранных согласно 5.3 инструментальных средств верификации критериям, сформулированным согласно 5.1.

6 Формализованное (машиночитаемое) описание формальной модели управления доступом

6.1 Для верификации формальная модель управления доступом должна иметь соответствующее ГОСТ Р 59453.1 формализованное (машиночитаемое) описание. Язык описания должен позволять выполнить требования к описанию формальной модели управления доступом и быть обеспечен инструментальными средствами для ее верификации, отвечающими критериям в соответствии с 5.3.

6.2 Если формальная модель управления доступом описана на математическом языке, то должен быть осуществлен перевод ее математического описания в формализованное (машиночитаемое) описание на языке, поддерживаемом формальными методами, реализуемыми выбранными в соответствии с 5.3 инструментальными средствами верификации.

6.3 При переводе математического описания в формализованное (машиночитаемое) описание формальной модели управления доступом должны быть последовательно описаны:

- элементы состояний абстрактного автомата в математическом описании формальной модели;

- правила перехода абстрактного автомата из состояний в состояния, при этом допустимо объединение нескольких правил в одно или разбиение некоторого правила на несколько с сохранением его свойств;

- условия выполнения политик управления доступом в состояниях абстрактного автомата и при переходах из состояний в состояния абстрактного автомата (условия безопасности), при этом могут быть добавлены недостающие для осуществления верификации условия, в целом составляющие условия верификации.

Примеры перевода элементов математического описания формальной модели управления доступом в формализованное (машиночитаемое) описание приведены в приложении А.

6.4 Если при переводе математического описания в формализованное (машиночитаемое) описание формальной модели управления доступом проводилась корректировка математического описания, то скорректированное математическое описание должно соответствовать ГОСТ Р 59453.1.

6.5 Если полученное в соответствии с 6.2 формализованное (машиночитаемое) описание формальной модели управления доступом имеет несоответствия ее математическому описанию, то должны быть представлены свидетельства согласованности и непротиворечивости этих описаний.

7 Верификация формализованного (машиночитаемого) описания формальной модели управления доступом

7.1 При верификации формальной модели управления доступом выбранные в соответствии с 5.3 инструментальные средства верификации должны быть применены к ее формализованному (машиночитаемому) описанию, полученному в соответствии с 6.1.

7.2 Верификация формализованного (машиночитаемого) описания формальной модели управления доступом с применением инструментальных средств должна состоять в выполнении следующих действий.

- должно быть осуществлено автоматическое доказательство непротиворечивости формальной модели и выполнения заданных в ее рамках условий безопасности (условий верификации) при наличии у инструментальных средств соответствующей функциональности, в противном случае должно быть выполнено интерактивное доказательство этих условий верификации;
- если доказаны все условия верификации, то она считается успешно завершенной, в противном случае должны быть идентифицированы недоказанные условия верификации и для каждого из них должны быть проанализированы причины, по которым их доказательство не было выполнено;
- если причинами невыполнения доказательства условий верификации являются ограничения инструментальных средств, то эти причины должны быть устранены, после чего доказательство должно быть осуществлено заново до успешного завершения верификации либо выявления дефектов описания формальной модели управления доступом.

Примечание — Возможными причинами невыполнения доказательства условий верификации формальной модели управления доступом и путями их устранения являются:

- если доказательство условий верификации не удалось выполнить из-за ограничений автоматического доказательства, реализуемого инструментальными средствами, то с их использованием должно быть осуществлено интерактивное доказательство этих условий верификации;
- если интерактивное доказательство не удалось выполнить из-за сложности доказываемых условий верификации, то при наличии соответствующей возможности должны быть осуществлены декомпозиция условий верификации на более простые условия верификации и автоматическое или интерактивное доказательство каждого из них в отдельности;
- если интерактивное доказательство условий верификации не удалось выполнить из-за ошибок в реализации инструментальных средств, то эти ошибки должны быть исправлены.

7.3 Если в процессе верификации выявлены дефекты описания формальной модели управления доступом, не позволяющие подтвердить ее непротиворечивость или выполнение заданных в ее рамках условий безопасности, то описание формальной модели должно быть скорректировано, при этом должно быть обеспечено соответствие описания формальной модели ГОСТ Р 59453.1, и ее верификация в соответствии с настоящим стандартом должна быть осуществлена заново.

Примечание — Формальная модель строится на основе некоторых априорных предположений, справедливость которых может быть обоснована неформально. Примером такого предположения может быть утверждение, что начальное состояние абстрактного автомата является безопасным (удовлетворяющим условиям безопасности), которое следует только из предположения об условиях функционирования средств защиты информации, реализующих политики управления доступом.

7.4 Результаты верификации не должны быть получены путем эксплуатации ошибок в инструментальных средствах верификации или благодаря наличию в описании формальной модели управления доступом логически противоречивых условий. Отсутствие таких дефектов должно быть подтверждено путем анализа инструментальных средств верификации, описания формальной модели и результатов ее верификации.

Примечание — Анализ на отсутствие ошибок в инструментальных средствах верификации может выполняться на основе их применения к предварительно сформированному тестовому набору формальных моделей управления доступом, включающему в том числе формальные модели, содержащие логически противоречивые условия. Рекомендуемым способом проверки является добавление отрицания к одному из логических условий, используемых в формальной модели управления доступом, и демонстрация невозможности доказать одно из свойств модели, зависящих от этого условия.

7.5 Результаты верификации формальной модели управления доступом должны быть представлены в воспроизводимом виде. При этом должны быть получены свидетельства об успешно завершенной верификации и описание конфигурации инструментальных средств верификации, достаточные для независимого воспроизведения выполненной верификации.

Приложение А
(справочное)

Примеры перевода элементов математического описания формальной модели управления доступом в формализованное (машиночитаемое) описание

А.1 Введение

В настоящем приложении приведены примеры перевода элементов математического описания формальной модели управления доступом в формализованное (машиночитаемое) описание на языке, поддерживаемом формальным методом Event-B.

А.2 Пример перевода элементов состояния абстрактного автомата

Пусть даны следующие элементы состояния абстрактного автомата математического описания формальной модели управления доступом:

S — множество субъектов доступа;

O — множество объектов;

C — множество контейнеров;

$E = O \cup C$ — множество объектов доступа (сущностей), где $O \cap C = \varnothing$;

$H_E: E \to 2^E$ — функция иерархии сущностей;

$RA = \{read_a, write_a\}$ — множество видов доступа, где $read_a$ — доступ на чтение, $write_a$ — доступ на запись;

$A \subset S \times (E \cup S) \times RA$ — множество реализуемых доступов субъектов доступа к сущностям и субъектам доступа;

$RR = \{read_r, write_r, execute_r, own_r\}$ — множество видов прав доступа;

$P \subset S \times (E \cup S) \times RR$ — множество реализуемых прав доступа субъектов доступа к сущностям и субъектам доступа;

$(LI, \leq)$ — решетка уровней целостности, где $\leq$ — отношение частичного порядка на множестве уровней целостности LI;

$(LC, \leq)$ — решетка уровней конфиденциальности, где $\leq$ — отношение частичного порядка на множестве уровней конфиденциальности LC;

$i_e: E \to LI$ — функция, задающая уровень целостности каждой сущности;

$i_s: S \to LI$ — функция, задающая уровень целостности каждого субъекта доступа;

$f_e: E \to LC$ — функция, задающая уровень конфиденциальности каждой сущности;

$f_s: S \to LC$ — функция, задающая уровень доступа каждого субъекта доступа.

В машиночитаемом описании формальной модели на языке, поддерживаемом формальным методом Event-B, для элементов неизменяемой части состояний используются статические множества (sets), константы (constants) и аксиомы (axioms). Изменяющиеся элементы состояний приводятся в блоке переменных (variables). В блоке инвариантов (invariants) — условий и требований на переменные, которые должны быть выполнены в каждом состоянии — каждой переменной задается тип.

```
context C0
sets
    AllEntitiesAndSubjects // множество всех субъектов доступа и сущностей
    AccessRights // множество видов доступа RR
    Accesses // множество видов прав доступа RA
    Integrity // уровни целостности решетки LI
    Confidentiality // уровни конфиденциальности решетки L
constants
    AllSubjects // множество всех возможных субъектов доступа
    AllEntities // множество всех возможных сущностей
    ReadR // право доступа read_r
    WriteR // право доступа write_r
    ExecuteR // право доступа execute_r
    OwnR // право доступа own_r
    ReadA // право доступа read_a
    WriteA // право доступа write_a
axioms
    @ AllEntitiesAndAllSubjectsTypes partition(AllEntitiesAndSubjects,
    AllSubjects, AllEntities)
    @AccessRightsTypes partition(AccessRights, {ReadR}, {WriteR}, {ExecuteR}, {OwnR})
    @AccessesTypes partition(Accesses, {ReadA}, {WriteA})
```

machine M0 sees C0
variables
Subjects // множество субъектов доступа S
Objects // множество объектов O
Containers // множество контейнеров C
Entities // множество сущностей E
EntityHierarchy // функция иерархии сущностей H_E
SubjectAccessRights // множество реализуемых прав доступа субъектов
// доступа к сущностям и субъектам доступа P
SubjectAccesses // множество реализуемых доступов субъектов
// доступа к сущностям и субъектам доступа A
EntityInt // функция, задающая уровень целостности
// каждой сущности i_e
SubjectInt // функция, задающая уровень целостности
// каждого субъекта доступа i_s
EntityCnf // функция, задающая уровень конфиденциальности
// каждой сущности f_e
SubjectCnf // функция, задающая уровень конфиденциальности
// каждого субъекта доступа f_s
invariants
@SubjectsType Subjects ⊂ AllSubjects
@EntitiesType Entities ⊂ AllEntities
@ObjectsAndContainersType partition(Entities, Objects, Containers)
@EntityHierarchyType EntityHierarchy ∈ Entities ⇸ ℙ(Entities)
@SubjectAccessRightsType SubjectAccessRights ∈ Subjects → (Subjects U Entities ↔ AccessRights)
@SubjectAccessesType SubjectAccesses ∈ Subjects → (Subjects U Entities ↔ Accesses)
@EntityIntType EntityInt ∈ Entities → ℙ(Integrity)
@SubjectIntType SubjectInt ∈ Subjects → ℙ(Integrity)
@EntityIntCnf EntityCnf ∈ Entities → ℙ(Confidentiality)
@SubjectCnfType SubjectCnf ∈ Subjects → ℙ(Confidentiality)

А.3 Пример перевода описания правила перехода абстрактного автомата из состояний в состояния

Заданное в математическом описании формальной модели управления доступом правило создания субъектом доступа объекта в контейнере имеет следующий вид. Параметры правила:

x — субъект доступа;

y — создаваемый объект;

z — контейнер, в котором создается объект;

yi — уровень целостности создаваемого объекта;

yc — уровень конфиденциальности создаваемого объекта.

Условия применения правила (ограничения на значения параметров правила и элементов состояния, к которому применяется правило):

$x \in S$ — субъект доступа функционирует в текущем состоянии абстрактного автомата;

$y \notin E$ — объект не существует в текущем состоянии абстрактного автомата;

$z \in C$ — контейнер существует в текущем состоянии абстрактного автомата;

$(x, z, write_a) \in A$ — субъект доступа обладает доступом на запись к контейнеру;

$(x, z, execute_r) \in P$ — субъект доступа обладает правом доступа на выполнение к контейнеру;

$yi \le \min(i_s(x), i_e(z))$ — уровень целостности создаваемого объекта не выше уровней целостности субъекта доступа и контейнера, в котором создается объект;

$yc = f_e(z) = f_s(x)$ — должны быть равны уровень доступа субъекта доступа и уровни конфиденциальности создаваемого объекта и контейнера, в котором создается объект.

Результаты применения правила (ограничения на значения элементов состояния, полученного в результате применения правила):

$E' = E \cup \{y\}$ — объект как сущность добавляется во множество сущностей в последующем состоянии абстрактного автомата;

$O' = O \cup \{y\}$ — объект добавляется во множество объектов;

$H_E'(z) = H_E(z) \cup \{y\}$ — объект добавляется в состав контейнера;

$H_E'(y) = \varnothing$ — созданный объект не включает другие объекты или контейнеры;

$P' = P \cup \{(x, y, own_r)\}$ — субъект доступа получает право доступа владения к созданному объекту;

$i_e'(y) = yi$ — для созданного объекта задается его уровень целостности;

$f_e'(y) = yc$ — для созданного объекта задается его уровень конфиденциальности.

В машиночитаемом описании на языке, поддерживаемом формальным методом Event-B, правило может задаваться следующим событием:

```
event create_object
    any // параметры
        x y z yi yc
    where // охранные условия выполнения события, соответствующие
          // условиям применения правила
        @grd1 x ∈ Subjects
        @grd2 y ∈ AllEntities \ Entities
        @grd3 z ∈ Containers
        @grd4 z ↦ WriteA ∈ SubjectAccesses(x)
        @grd5 z ↦ ExecuteR ∈ SubjectAccessRights(x)
        @grd6 yi ⊂ EntityInt(z) ∧ yi ⊆ SubjectInt(x)
        @grd7 yc = EntityCnf(z) ∧ yc = SubjectCnf(x)
            @grd8 z ∈ dom(EntityHierarchy)
    then // действия по изменению значений переменных состояния
         // в результате срабатывания события, соответствующие
         // результатам применения правила
        @act1 Entities ≔ Entities U {y}
        @act2 Objects ≔ Objects U {y}
        @act3-4 EntityHierarchy(z) ≔ EntityHierarchy(z) U {y}
        @act5 SubjectAccessRights(x) ≔ SubjectAccessRights(x) U {y ↦ OwnR}
        @act6 EntityInt(y) ≔ yi
        @act7 EntityCnf(y) :≔ yc
    end
```

А.4 Пример перевода условия безопасности

Заданные в математическом описании формальной модели управления доступом ограничения на уровни целостности сущностей в составе контейнеров определяются следующим образом: для сущностей x, y ∈ E, если $x \in H_E(y)$, то $i_e(x) \le i_e(y)$ (уровень целостности сущности не выше уровня целостности контейнера, в котором она содержится). В машиночитаемом описании на языке, поддерживаемом формальным методом Event-B, ограничения на уровни целостности задаются инвариантом:

```
invariants
    @EntityHierarchy1
        ∀x, y · x ∈ Entities ∧ y ∈ Entities ∧ x ∈ dom(EntityHierarchy)
                ⇒ EntityInt(x) ⊂ EntityInt(y)
```

УДК 004.056:006.354 ОКС 35.030

Ключевые слова: защита информации, формальная модель управления доступом, верификация формальной модели управления доступом, средство защиты информации, инструментальное средство верификации формальной модели управления доступом

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 23.04.2021. Подписано в печать 28.04.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru