"ГОСТ Р 59453.1-2021. Национальный стандарт Российской Федерации. Защита информации. Формальная модель управления доступом. Часть 1. Общие положения" (утв. и введен в действие Приказом Росстандарта от 22.04.2021 N 270-ст)

Утвержден и введен в действие
Приказом Федерального
агентства по техническому
регулированию и метрологии
от 22 апреля 2021 г. N 270-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАЩИТА ИНФОРМАЦИИ

ФОРМАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

ЧАСТЬ 1

ОБЩИЕ ПОЛОЖЕНИЯ

**Information protection. Formal access control model.
Part 1. General principles**

ГОСТ Р 59453.1-2021

ОКС 35.030

**Дата введения
1 июня 2021 года**

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Обществом с ограниченной ответственностью "РусБИТех-Астра" (ООО "РусБИТех-Астра")

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. N 270-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.gost.ru)

Введение

Формальные модели управления доступом используются для обеспечения доверия к средствам защиты информации, реализующим политики управления доступом, уменьшения числа недостатков при проектировании этих средств.

Формальное моделирование управления доступом, как правило, основывается на описании абстрактного автомата как математической модели дискретных устройств. Применение абстрактного автомата при моделировании управления доступом базируется на том, что абстрактный автомат может рассматриваться в качестве непосредственного прототипа средства защиты информации. Кроме моделирования на основе абстрактного автомата, могут использоваться темпоральные логики, сети Петри или другие способы.

Целью настоящего стандарта является определение критериев, которым должны соответствовать описания формальных моделей управления доступом. Требования к порядку разработки формальных моделей управления доступом и порядку разработки на их основе средств защиты информации, реализующих политики управления доступом, выходят за рамки настоящего стандарта и будут определены другими документами по стандартизации.

1 Область применения

Настоящий стандарт устанавливает критерии, которым должны соответствовать описания формальных моделей управления доступом, на основе которых разрабатываются средства защиты информации, реализующие политики управления доступом (дискреционная, ролевая, мандатная или другие виды политик 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 использована нормативная ссылка на следующий стандарт:

ГОСТ Р 53113.1 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. 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 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.

3.2 **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.

3.3 **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.

3.4 **объект доступа**: Компонент среды функционирования средства защиты информации, доступ к которому регламентируется политиками управления доступом.

Примечание - В формальных моделях управления доступом используются следующие виды объектов доступа:

- объект: пассивный атомарный компонент [например, единица информационного ресурса, файл, сокет, запись и (или) иной] среды функционирования средства защиты информации, доступ к которому регламентируется политиками управления доступом, к частям которого по отдельности управление доступом не осуществляется;

- контейнер: пассивный составной компонент [например, единица информационного ресурса, каталог, том, устройство, кластер и (или) иной] среды функционирования средства защиты информации, доступ к которому регламентируется политиками управления доступом, состоящий из объектов или контейнеров, к которым по отдельности возможно осуществление управления доступом.

При этом сущностью называется пассивный компонент среды функционирования средства защиты информации, являющийся объектом или контейнером.

3.5 **объект доступа, ассоциированный функционально с субъектом доступа**: Объект доступа, содержание информации в котором влияет на функциональность субъекта доступа, и информационный поток по памяти к этому объекту от другого субъекта доступа позволяет второму субъекту доступа получить управление первым субъектом доступа.

Примечание - Под управлением субъектом доступа другим субъектом доступа, как правило, рассматривается возможность второго субъекта доступа инициировать с заданными им параметрами действия первого субъекта доступа [например, получение доступа к заданному объекту доступа, изменение прав доступа к заданному объекту доступа, создание информационного потока между заданными объектами доступа и (или) иные]. В среде функционирования средства защиты информации объектом доступа, ассоциированным функционально с субъектом доступа, может быть, например, исполняемый файл, из которого активизирован процесс операционной системы, являющийся этим субъектом доступа.

3.6 **политика управления доступом**: Совокупность правил, подлежащих реализации средством защиты информации и регламентирующих предоставление доступа между компонентами среды функционирования этого средства защиты информации.

Примечание - В качестве компонента среды функционирования средства защиты информации, как правило, рассматривается объект или субъект доступа. При этом доступом между компонентами среды функционирования средства защиты информации является доступ субъекта доступа к субъекту или объекту доступа.

3.7 **политика дискреционного управления доступом**: Политика управления доступом, при реализации которой задается матрица доступов, строки которой соответствуют субъектам доступа (учетным записям пользователей), столбцы - объектам или субъектам доступа, ячейки - множеству прав доступа соответствующего строке субъекта доступа к соответствующему столбцу объекту или другому субъекту доступа; субъект доступа может получить доступ к объекту или другому субъекту доступа только в случае, когда выполняется следующее правило: в ячейке матрицы доступов, соответствующей субъекту доступа и объекту или другому субъекту доступа, содержится соответствующее право доступа.

Примечание - Матрица доступов может быть задана эквивалентными способами: списки контроля доступа, списки привилегий, граф прав доступа или другие способы.

3.8 **политика мандатного контроля целостности**: Политика управления доступом, при реализации которой задаются классификационные метки (уровни целостности): каждому объекту и субъекту доступа присваивается уровень целостности; субъект доступа может получить доступ к объекту доступа или другому субъекту доступа только в случае, когда выполняются следующие правила:

- при получении доступа на запись к объекту доступа уровень целостности субъекта доступа должен быть не ниже уровня целостности объекта доступа;

- доступ субъекта доступа к объекту или другому субъекту доступа не приводит к получению субъектом доступа управления некоторым субъектом доступа, уровень целостности которого не сравним или выше уровня целостности первого субъекта доступа.

Примечание - Уровень целостности объекта доступа, как правило, отражает степень уверенности в целостности содержащейся в нем информации. Уровень целостности субъекта доступа, как правило, соответствует его полномочиям по доступу к объектам доступа в зависимости от их уровней целостности, а также отражает степень уверенности в корректности его функциональности. Классификационные метки могут быть не сравнимы друг с другом, например, при использовании для их задания неиерархических категорий.

3.9 **политика мандатного управления доступом**: Политика управления доступом, при реализации которой задаются классификационные метки (уровни конфиденциальности, уровни доступа): каждому объекту доступа присваивается уровень конфиденциальности, каждому субъекту доступа присваивается уровень доступа (являющийся элементом множества уровней конфиденциальности); субъект доступа может получить доступ к объекту или другому субъекту доступа только в случае, когда выполняются следующие правила:

- при получении доступа на чтение к объекту доступа уровень доступа субъекта доступа должен быть не ниже уровня конфиденциальности объекта доступа;

- при получении доступа на запись к объекту доступа уровень доступа субъекта доступа должен быть не выше уровня конфиденциальности объекта доступа;

- доступ субъекта доступа к объекту доступа или другому субъекту доступа не приводит к возникновению скрытого канала от объекта доступа к другому объекту доступа, первый из которых обладает не сравнимым или более высоким уровнем конфиденциальности, чем у второго объекта доступа.

Примечание - Уровень конфиденциальности объекта доступа, как правило, отражает степень конфиденциальности содержащейся в нем информации. Уровень доступа субъекта доступа, как правило, соответствует степени его полномочий по доступу к объектам доступа в зависимости от их уровней конфиденциальности. Классификационные метки могут быть не сравнимы друг с другом, например, при использовании для их задания неиерархических категорий.

3.10 **политика ролевого управления доступом**: Политика управления доступом, при реализации которой задаются роли, каждая из которых представляет собой поименованное множество прав доступа к объектам доступа или субъектам доступа; каждому субъекту доступа ставится в соответствие множество разрешенных для него ролей; субъект доступа может получить доступ к объекту или другому субъекту доступа только в случае, когда выполняется следующее правило: во множестве соответствующих субъекту доступа ролей имеется роль, во множестве прав доступа к объектам или субъектам доступа которой содержится соответствующее право доступа к объекту или субъекту доступа.

3.11 **право доступа**: Совокупность установленных политиками управления доступом

правил, регламентирующих предоставление доступа субъекту доступа к объекту или другому субъекту доступа.

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

3.13 **среда функционирования средства защиты информации**: Среда, в которой функционирует средство защиты информации.

Примечание - Поскольку реализуемые средством защиты информации политики управления доступом, как правило, регламентируют предоставление доступа между компонентами самого этого средства и компонентами среды его функционирования, то в настоящем стандарте предполагается, что среда функционирования средства защиты информации включает само это средство.

3.14 **субъект доступа**: Активный компонент среды функционирования средства защиты информации, доступы которого регламентируются политиками управления доступом.

3.15 **субъект доступа непривилегированный**: Субъект доступа, функционирующий от имени учетной записи непривилегированного пользователя.

Примечание - Как правило, каждому субъекту доступа (например, процессу) средством защиты информации ставится в соответствие учетная запись пользователя, от имени которой он функционирует (например, учетная запись пользователя, указанная им при начале его работы со средством защиты информации). Если средством защиты информации явно не используются учетные записи пользователей, то можно считать, что для всех субъектов доступа задана единая учетная запись пользователя (например, "Системный пользователь").

3.16 **субъект доступа привилегированный**: Субъект доступа, функционирующий от имени учетной записи привилегированного пользователя.

3.17 **условие безопасности**: Ограничение, учитываемое в формальной модели управления доступом, необходимое для реализуемой средством защиты информации политики управления доступом.

Примечание - Условие безопасности в зависимости от реализуемой средством защиты информации политики управления доступом может накладывать ограничение, например, на права доступа субъекта доступа к объектам доступа с учетом учетной записи пользователя, от имени которой этот субъект доступа функционирует, или на информационные потоки между объектами или субъектами доступа с учетом их классификационных меток.

3.18 **учетная запись пользователя**: Хранящаяся в среде функционирования средства защиты информации информация о пользователе этой среды, включающая информацию о его полномочиях [привилегиях, ролях, правах доступа и (или) иных] в соответствии с политиками управления доступом.

3.19 **учетная запись непривилегированного пользователя**: Учетная запись пользователя, не имеющего полномочия по управлению средством защиты информации.

3.20 **учетная запись привилегированного пользователя**: Учетная запись пользователя,

имеющего полномочия по управлению средством защиты информации.

3.21 **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.

4 Общие положения

4.1 Описание формальной модели управления доступом, на основе которой разрабатывается средство защиты информации, реализующее политики управления доступом, должно соответствовать установленным в настоящем стандарте критериям.

4.2 В формальной модели управления доступом должны быть определены виды реализуемых средством защиты информации политик управления доступом (дискреционная, ролевая, мандатная или другие виды политик управления доступом).

4.3 Содержание описания формальной модели управления доступом должно включать описание состояний и правил перехода между состояниями абстрактного автомата, соответствующего заданным в 4.2 политикам управления доступом. Это описание должно быть дано как минимум с использованием терминов: объект доступа (объект, контейнер, сущность), учетная запись пользователя, субъект доступа, доступ, право доступа, информационный поток.

4.4 Формальная модель управления доступом должна включать описание условий безопасности, выполнение которых в абстрактном автомате указывает на реализацию заданных в соответствии с 4.2 политик управления доступом. Уверенность в корректности формальной модели управления доступом должна быть достигнута математическим (формальным) доказательством того, что в ней не содержится противоречий, т.е. в абстрактном автомате выполняются условия безопасности.

4.5 Язык описания формальной модели управления доступом должен быть математическим или формализованным и должен допускать полную независимую от разработчика формальной модели проверку корректности ее описания, заданных в ней условий безопасности, а также всех выполненных в модели доказательств.

Примечание - Для формализованного (машиночитаемого) описания формальной модели управления доступом можно использовать формальные методы, например, Alloy, ASM, B, Event-B, TLA+, VDM-SL, Z, языки которых позволяют строить абстрактные автоматные модели.

4.6 Для описанных в соответствии с 4.4 условий безопасности должна быть показана их взаимосвязь с режимами функционирования средства защиты информации, разрабатываемого согласно выполненному в соответствии с 4.3 описанию абстрактного автомата и реализующего заданные в соответствии с 4.2 политики управления доступом.

Пример - Использование математического языка для задания функции прав доступа ролей.

RR = {readr, writer, executer, ownr} - множество видов прав доступа, где readr - право доступа на чтение, writer - право доступа на запись, executer - право доступа на выполнение,

own_r - право доступа на владение;

E - множество объектов доступа (сущностей);

R - множество ролей;

PA: $R \to 2^{E \times RR}$ ***- функция прав доступа ролей к сущностям, задающая для каждой роли*** $p \in R$ ***множество прав доступа этой роли к сущностям*** $PA(p) \subseteq E \times RR$.

5 Описание состояний в рамках формальной модели управления доступом

5.1 В рамках формальной модели управления доступом формальное описание состояний абстрактного автомата должно включать:

- множество учетных записей пользователей;

- множество субъектов доступа;

- множество объектов доступа (объектов, контейнеров, сущностей);

- заданное на множестве объектов доступа отношение иерархии;

- множество реализуемых доступов субъектов к объектам доступа и используемые для задания доступов множества, функции (отношения);

- множество реализуемых прав доступа субъектов к объектам или субъектам доступа и используемые для задания прав доступа (непосредственно или с использованием групп, ролей, типов, атрибутов) множества, функции (отношения);

- множество информационных потоков;

- условия внутренней и взаимной корректности (согласованности) используемых для описания состояний абстрактного автомата множеств, функций (отношений).

Примечание - Иерархией на множестве объектов доступа (объектов, контейнеров, сущностей) в общем случае считается заданное на нем отношение частичного порядка. При этом в формальных моделях управления доступом на это отношение накладываются соответствующие технологиям, как правило, применяемым в файловых системах, дополнительные условия, такие как: объектам не могут быть подчинены в иерархии другие сущности, или каждый контейнер может быть подчинен в иерархии строго одному другому контейнеру.

Пример - U - множество учетных записей пользователей;

S - множество субъектов доступа;

user: $S \to U$ ***- функция, задающая для каждого субъекта доступа учетную запись пользователя, от имени которой он функционирует;***

O - множество объектов;

C - множество контейнеров;

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

Не: $E \to 2^E$ *- функция иерархии сущностей, используемая для задания отношения иерархии на множестве сущностей (объектов доступа), где для каждого объекта* $o \in O$ *верно* $HE(o) = \varnothing$ *(в иерархии сущностей только контейнеры могут содержать другие контейнеры или объекты);*

RA = {read$_a$, write$_a$} - множество видов доступа, где read$_a$ - доступ на чтение, write$_a$ - доступ на запись;

$A \subseteq S \times E \times RA$ *- множество реализуемых доступов субъектов доступа к сущностям (объектам доступа);*

RR = {read$_r$, write$_r$, execute$_r$, own$_r$} - множество видов прав доступа;

$P \subseteq S \times (E \cup S) \times RR$ *- множество реализуемых прав доступа субъектов доступа к сущностям (объектам доступа) или субъектам доступа;*

RF = {write$_m$, write$_t$} - множество видов информационных потоков, где write$_m$ - информационный поток по памяти, write$_t$ - информационный поток по времени (информационные потоки по памяти и по времени рассматриваются в соответствии с ГОСТ Р 53113.1);

$F \subseteq (E \cup S) \times (E \cup S) \times RF$ *- множество информационных потоков;*

$P \cap (S \times S \times RR) \subseteq \{(s, s', own_r) : s, s' \in S\}$ *- условие корректности множества реализуемых прав доступа субъектов к субъектам доступа (субъекты доступа могут иметь к друг другу только право доступа владения).*

5.2 Если заданные в соответствии с 4.2 политики управления доступом включают политику дискреционного управления доступом, то формальное описание состояний абстрактного автомата в дополнение к 5.1 должно включать матрицу доступов (в виде таблицы, списка контроля доступа, списка привилегий, графа прав доступа или другого способа ее задания).

Пример - M - матрица доступов, где $M[s, o] \subseteq RR$ *- права доступа субъекта доступа* $s \in S$ *к объекту* $o \in O$.

5.3 Если заданные в соответствии с 4.2 политики управления доступом включают политику ролевого управления доступом, то формальное описание состояний абстрактного автомата в дополнение к 5.1 должно включать:

- множество ролей;

- множества, функции (отношения), используемые для задания прав доступа (привилегий) ролей к субъектам и объектам доступа;

- заданное на множестве ролей отношение иерархии;

- множества, функции (отношения), используемые для задания каждой учетной записи пользователя разрешенных для нее ролей (разрешенных для обладания субъектами доступа, функционирующими от имени этой учетной записи пользователя);

- множества, функции (отношения), используемые для задания текущих ролей, которыми обладают субъекты доступа.

Примечание - Иерархией на множестве ролей в общем случае считается заданное на нем отношение частичного порядка. При этом в формальных моделях управления доступом на это отношение, как правило, накладываются дополнительные условия, такие как: если для учетной записи пользователя разрешена некоторая роль, то для нее должны быть разрешены все роли, подчиненные в иерархии этой роли.

Пример - R - множество ролей;

Hr: $R \to 2^R$ ***- функция иерархии ролей;***

PA: $R \to 2^{(E \cup S) \times RR}$ ***- функция прав доступа ролей;***

UA: $U \to 2^R$ ***- функция ролей, разрешенных для учетных записей пользователей;***

roles: $S \to 2^R$ ***- функция текущих ролей субъектов доступа, при этом в каждом состоянии абстрактной системы для каждого субъекта доступа*** $s \in S$ ***выполняется условие*** $roles(s) \subseteq UA(user(s))$.

5.4 Если заданные в соответствии с 4.2 политики управления доступом включают политику мандатного контроля целостности, то формальное описание состояний абстрактного автомата в дополнение к 5.1 должно включать:

- решетку уровней целостности [каждый элемент которой является комбинацией иерархических и (или) неиерархических категорий], функции (отношения), используемые для задания уровней целостности учетных записей пользователей, субъектов и объектов доступа;

- множества учетных записей привилегированных и непривилегированных пользователей;

- множества привилегированных и непривилегированных субъектов доступа;

- множества, функции (отношения), используемые для задания объектов доступа, функционально ассоциированных с субъектами доступа;

- множества, функции (отношения), используемые для задания субъектов доступа, управляемых другими субъектами доступа.

Пример - (LI, <=) - решетка уровней целостности, где <= - отношение частичного порядка на множестве уровней целостности LI;

$L_U \subseteq U$ ***- множество учетных записей привилегированных пользователей,*** $N_U \subseteq U$ ***- множество учетных записей непривилегированных пользователей, где*** $L_U \cap N_U = \varnothing$, $L_U \cup N_U = U$;

$L_S \subseteq S$ ***- множество привилегированных субъектов доступа,*** $N_S \subseteq S$ ***- множество непривилегированных субъектов доступа, где*** $L_S \cap N_S = \varnothing$, $L_S \cup N_S = S$;

i_U: $U \to LI$ ***- функция, задающая уровень целостности каждой учетной записи пользователя;***

i_E: $E \to LI$ ***- функция, задающая уровень целостности каждого объекта доступа (сущности);***

i_S: $S \to LI$ ***- функция, задающая уровень целостности каждого субъекта доступа;***

$[s] \subset E$ ***- множество сущностей, функционально ассоциированных с субъектом доступа*** $s \in S$;

control: $S \to 2^S$ ***- функция, задающая для каждого субъекта доступа множество управляемых им субъектов доступа.***

5.5 Если заданные в соответствии с 4.2 политики управления доступом включают политику мандатного управления доступом, то формальное описание состояний абстрактного автомата в дополнение к 5.1 должно включать:

- решетку уровней конфиденциальности [каждый элемент которой является комбинацией иерархических и (или) неиерархических категорий], используемые для задания уровней доступа учетных записей пользователей и субъектов доступа, уровней конфиденциальности объектов доступа функции (отношения);

- множества, функции (отношения), используемые для задания объектов доступа (контейнеров), доступ к содержащимся в которых объектам доступа субъектам доступа может быть разрешен без учета уровней конфиденциальности таких объектов доступа (контейнеров).

Пример - (LC, <=) - решетка уровней конфиденциальности, где <= - отношение

частичного порядка на множестве уровней конфиденциальности LC;

f_U: $U \to LC$ - *функция, задающая уровень доступа каждой учетной записи пользователя;*

f_E: $E \to LC$ - *функция, задающая уровень конфиденциальности каждого объекта доступа (сущности);*

f_S: $S \to LC$ - *функция, задающая уровень доступа каждого субъекта доступа;*

CCR: $C \to \{true, false\}$ - *функция, задающая способ доступа к сущностям внутри контейнеров с учетом их уровней конфиденциальности, где если доступ к сущностям, содержащимся внутри контейнера* $c \in C$, *разрешен без учета уровня его конфиденциальности, то по определению выполняется равенство CCR(c) = false, в противном случае выполняется равенство CCR(c) = true.*

6 Описание правил перехода из состояний в состояния в рамках формальной модели управления доступом

6.1 В рамках формальной модели управления доступом описание абстрактного автомата должно включать правила его перехода из состояний в состояния (команды, операции, функции перехода), содержащие параметры каждого правила, условия (предусловия) и результаты (постусловия) его применения. Должны быть формально описаны правила:

- для создания, удаления учетных записей пользователей, объектов или субъектов доступа;

- для изменения прав доступа учетных записей пользователей и (или) субъектов доступа к объектам или субъектам доступа;

- для получения, удаления доступов субъектов доступа к объектам или субъектам доступа;

- для изменения иерархии объектов доступа;

- для создания информационных потоков.

Примечание - Совокупность инициирующих переходы абстрактного автомата из состояний в состояния правил, команд, операций, функций со всеми возможными наборами их параметров рассматриваются как входной алфавит абстрактного автомата. При описании правил перехода абстрактного автомата из состояний в состояния стремятся обеспечить их согласованность с режимами функционирования средства защиты информации таким образом, чтобы каждому наблюдаемому состоянию или последовательности состояний средства защиты информации, связанного с реализацией политик управления доступом, можно было поставить в соответствие правило или последовательность правил перехода абстрактного автомата из состояний в состояния.

6.2 Если заданные в соответствии с 4.2 политики управления доступом включают только политику дискреционного управления доступом, то перечисленных в 6.1 правил перехода

абстрактного автомата из состояний в состояния достаточно для ее описания.

6.3 Если заданные в соответствии с 4.2 политики управления доступом включают политику ролевого управления доступом, то в дополнение к 6.1 должны быть формально описаны правила перехода абстрактного автомата из состояний в состояния:

- для создания, удаления ролей;

- для изменения иерархии ролей;

- для задания и (или) изменения прав доступа (привилегий) ролей;

- для изменения множеств ролей, разрешенных для учетных записей пользователей;

- для изменения множеств текущих ролей, которыми обладают субъекты доступа.

6.4 Если заданные в соответствии с 4.2 политики управления доступом включают политику мандатного контроля целостности, то в дополнение к 6.1 должны быть формально описаны правила перехода абстрактного автомата из состояний в состояния:

- для задания и (или) изменения уровней целостности учетных записей пользователей или субъектов доступа;

- для задания и (или) изменения уровней целостности объектов доступа;

- для получения субъектами доступа управления другими субъектами доступа за счет использования информационных потоков по памяти к объектам доступа, функционально ассоциированным с субъектами доступа.

6.5 Если заданные в соответствии с 4.2 политики управления доступом включают политику мандатного управления доступом, то в дополнение к 6.1 должны быть формально описаны правила перехода абстрактного автомата из состояний в состояния:

- для задания и (или) изменения уровней доступа учетных записей пользователей или субъектов доступа;

- для задания и (или) изменения уровней конфиденциальности объектов доступа.

Примеры

1 Правило создания субъектом доступа объекта в контейнере.

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:

$x \in S$ *- 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 <= 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:

$E' = E \cup \{y\}$ *- объект добавляется во множество объектов доступа (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.

2 Правило получения субъектом доступа доступа на запись к сущности.

Параметры правила:

x - субъект доступа;

y - сущность.

Условия применения правила:

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

$y \in E$ ***- сущность существует в текущем состоянии абстрактного автомата;***

$p \in roles(x)$, $(y, write_r) \in PA(p)$ ***- у субъекта доступа имеется текущая роль, обладающая правом доступа на запись к сущности;***

$i_e(y) <= i_s(x)$ ***- уровень целостности сущности не выше уровня целостности субъекта доступа;***

$f_r(y) = f_s(x)$ ***- уровень конфиденциальности сущности равен уровню доступа субъекта доступа.***

Результаты применения правила:

$A' = A \cup \{(x, y, write_a)\}$ ***- во множество реализуемых доступов в последующем состоянии абстрактного автомата добавляется доступ на запись субъекта доступа к сущности.***

3 Правило захвата управления субъектом доступа другим субъектом доступа.

Параметры правила:

x, y - субъекты доступа;

z - сущность.

Условия применения правила:

$x, y \in S$ ***- субъекты доступа функционируют в текущем состоянии абстрактного автомата;***

$z \in E$ ***- сущность существует в текущем состоянии абстрактного автомата;***

$z \in [y]$ ***- сущность является функционально ассоциированной с субъектом доступа;***

$(x, z, write_m) \in F$ - *существует информационный поток по памяти от субъекта доступа к сущности.*

Результаты применения правила:

$control'(x) = control(x) \cup \{y\}$ - *в последующем состоянии абстрактного автомата субъект доступа y добавляется во множество субъектов доступа, управляемых субъектом доступа x.*

4 Правило создания субъектом доступа информационного потока между двумя сущностями.

Параметры правила:

y - субъект доступа;

x, z - сущности.

Условия применения правила:

$y \in S$ - *субъект доступа функционирует в текущем состоянии абстрактного автомата;*

$x, z \in E$ - *сущности существуют в текущем состоянии абстрактного автомата;*

$(y, x, read_a) \in A$ - *субъект доступа имеет доступ на чтение к сущности;*

$(y, z, \alpha) \in F$, *где* $\alpha \in RF$ - *субъект доступа имеет информационный поток по памяти или по времени к сущности.*

Результаты применения правила:

$F' = F \cup \{(x, z, \alpha)\}$ - *если субъект доступа имел информационный поток по памяти к сущности z, то между сущностями в последующем состоянии абстрактного автомата создается информационный поток по памяти, в противном случае создается информационный поток по времени.*

7 Доказательство выполнения условий безопасности

7.1 В рамках формальной модели управления доступом в соответствии с политиками управления доступом, заданными в соответствии с 4.2, формальное описание абстрактного автомата должно включать:

- условия безопасности состояний абстрактного автомата;

- условия безопасности переходов из состояний в состояния абстрактного автомата;

- математическое (формальное) доказательство выполнения условий безопасности во всех состояниях и при всех переходах из состояний в состояния на всех траекториях функционирования абстрактного автомата, начинающихся с состояний, удовлетворяющих условиям безопасности.

7.2 Если заданные в соответствии с 4.2 политики управления доступом включают политику дискреционного управления доступом, то описание абстрактного автомата в дополнение к 7.1 должно включать:

а) условия безопасности абстрактного автомата, реализующего дискреционное управление доступом, включающие как минимум ограничения:

1) на права доступа субъектов доступа (учетных записей пользователей) к объектам или субъектам доступа;

2) информационные потоки;

б) математическое (формальное) доказательство того, что при выполнении условий безопасности абстрактного автомата, реализующего дискреционное управление доступом, в абстрактном автомате невозможно получение субъектом доступа не соответствующего условиям безопасности права доступа или доступа к объекту или субъекту доступа.

Пример - $P = LP \cup NP$, ***где*** $LP \cap NP = \varnothing$ ***- множество реализуемых прав доступа субъектов доступа к субъектам или объектам доступа (сущностям) состоит из двух непересекающихся множеств, соответствующих (LP) и не соответствующих (NP) условиям безопасности;***

$A = LA \cup NA$, ***где*** $LA \cap NA = \varnothing$ ***- множество реализуемых доступов субъектов доступа к сущностям состоит из двух непересекающихся множеств, соответствующих (LA) и не соответствующих (NA) условиям безопасности;***

Для субъекта доступа $s \in S$, ***сущности*** $e \in E$, ***права доступа*** $\alpha_r \in RR$, ***доступа*** $\alpha_a \in RA$ ***верно*** $(s, e, \alpha_r) \in LP$, $(s, e, \alpha_a) \in LA$ ***- условие безопасности, заключающееся в том, что в состояниях абстрактного автомата каждый субъект доступа может обладать к сущности только соответствующим правом доступа (из множества LP) или доступом (из множества LA).***

7.3 Если заданные в соответствии с 4.2 политики управления доступом включают политику ролевого управления доступом, то описание абстрактного автомата в дополнение к 7.1 должно включать:

а) условия безопасности абстрактного автомата, реализующего ролевое управление доступом, включающие как минимум ограничения:

1) на роли, разрешенные для учетных записей пользователей;

2) текущие роли, которыми обладают субъекты доступа;

3) права доступа (привилегии) ролей;

4) отношения подчиненности в иерархии ролей;

5) права доступа субъектов доступа к объектам или субъектам доступа, которыми они могут обладать с использованием текущих ролей;

6) информационные потоки;

б) математическое (формальное) доказательство того, что при выполнении условий безопасности абстрактного автомата, реализующего ролевое управление доступом, в абстрактном автомате невозможно получение субъектом доступа не соответствующего условиям безопасности права доступа (с использованием текущей роли, которой обладает субъект доступа) или доступа к объекту или субъекту доступа.

Пример - Для субъекта доступа $s \in S$, ***роли*** $p \in R$, ***сущности*** $e \in E$, ***права доступа*** $\alpha_r \in RR$ ***верно*** $(s, e, \alpha_r) \in LP$, ***когда*** $p \in roles(s)$, $(e, \alpha_r) \in PA(p)$ ***- субъект доступа может обладать с использованием текущей роли только правом доступа к сущности, соответствующим условиям безопасности.***

7.4 Если заданные в соответствии с 4.2 политики управления доступом включают политику мандатного контроля целостности, то описание абстрактного автомата в дополнение к 7.1 должно включать:

а) условия безопасности абстрактного автомата, реализующего мандатный контроль целостности, включающие как минимум ограничения:

1) на уровни целостности субъектов доступа в зависимости от уровней целостности учетных записей пользователей, от имени которых они функционируют;

2) уровни целостности объектов доступа в составе объектов доступа (контейнеров);

3) уровни целостности для объектов доступа, функционально ассоциированных с субъектами доступа, в зависимости от уровней целостности субъектов доступа;

4) возможности управления одним субъектом доступа другим субъектом доступа в зависимости от их уровней целостности;

5) информационные потоки;

б) математическое (формальное) доказательство того, что при выполнении условий безопасности абстрактного автомата, реализующего мандатный контроль целостности, в абстрактном автомате невозможно получение непривилегированным субъектом доступа управления другим субъектом доступа в случае, когда уровень целостности первого субъекта

доступа не сравним или меньше уровня целостности второго субъекта доступа.

Примеры

1 Ограничения на уровни целостности субъектов доступа в зависимости от уровней целостности учетных записей пользователей.

Для субъекта доступа $s \in S$ ***верно неравенство*** $i_S(s) <= i_U(user(s))$ ***- уровень целостности субъекта доступа не выше уровня целостности учетной записи пользователя, от имени которой он функционирует.***

2 Ограничения на уровни целостности объектов доступа (сущностей) в составе объектов доступа (контейнеров).

Для сущностей $x, y \in E$ ***, если*** $x \in H_E(y)$ ***, то*** $i_E(x) <= i_E(y)$ ***- уровень целостности сущности не выше уровня целостности контейнера, в котором она содержится.***

3 Ограничения на уровни целостности для сущностей, функционально ассоциированных с субъектами доступа.

Если $e \in [s]$ ***, то выполняется неравенство*** $i_S(s) <= i_E(e)$ ***- если сущность функционально ассоциирована с субъектом доступа, то уровень целостности субъекта доступа не выше уровня целостности сущности.***

4 Ограничения на уровни целостности при управлении субъектами доступа другими субъектами доступа.

Для каждых субъектов доступа $x, y \in S$ ***таких, что*** $y \in control(x)$ ***, верно*** $i_S(y) <= i_S(x)$ ***- если субъект доступа управляется другим субъектом доступа, то уровень целостности первого субъекта доступа не выше уровня целостности второго субъекта доступа.***

5 Ограничения на информационные потоки.

Для каждых непривилегированного субъекта доступа $x \in N^S$ ***, субъекта доступа*** $y \in S$ ***и сущности*** $e \in E$ ***таких, что*** $e \in [y]$ ***и*** $(x, e, write_m) \in F$ ***, верно неравенство*** $i_S(y) <= i_S(x)$ ***- если непривилегированным субъектом доступа реализован информационный поток по памяти к сущности, функционально ассоциированной с другим субъектом доступа, то его уровень целостности не выше уровня целостности непривилегированного субъекта доступа;***

для каждого информационного потока $(x, y, write_m) \in F$ ***справедливо неравенство*** $i_E(y) <= i_E(x)$ ***- разрешены только информационные потоки по памяти, когда сущность-приемник имеет уровень целостности не выше уровня целостности сущности-источника.***

7.5 Если заданные в соответствии с 4.2 политики управления доступом включают политику мандатного управления доступом, то описание абстрактного автомата в дополнение к 7.1 должно включать:

а) условия безопасности абстрактного автомата, реализующего мандатное управление доступом, включающие как минимум ограничения:

1) на уровни доступа субъектов доступа в зависимости от уровней доступа учетных записей пользователей, от имени которых они функционируют;

2) уровни конфиденциальности объектов доступа в составе объектов доступа (контейнеров);

3) уровни конфиденциальности для объектов доступа, функционально ассоциированных с субъектами доступа, в зависимости от уровней доступа субъектов доступа;

4) возможности управления одним субъектом доступа другим субъектом доступа в зависимости от их уровней доступа;

5) информационные потоки;

б) математическое (формальное) доказательство того, что при выполнении условий безопасности абстрактного автомата, реализующего мандатное управление доступом, в абстрактном автомате невозможно несанкционированное создание субъектом(ами) доступа скрытого канала от объекта доступа к объекту доступа, когда уровень конфиденциальности первого объекта доступа не сравним или выше уровня конфиденциальности второго объекта доступа.

Примеры

1 Ограничения на уровни доступа субъектов доступа в зависимости от уровней доступа учетных записей пользователей.

Для субъекта доступа $s \in S$ ***верно неравенство*** $f_s(s) <= f_u(user(s))$ ***- уровень доступа субъекта доступа не выше уровня доступа учетной записи пользователя, от имени которой он функционирует.***

2 Ограничения на уровни конфиденциальности объектов доступа (сущностей) в составе объектов доступа (контейнеров).

Для сущностей $x, y \in E$, ***если*** $x \in H_E(y)$, ***то*** $f_e(x) <= f_e(y)$ ***- уровень конфиденциальности сущности не выше уровня конфиденциальности контейнера, в котором она содержится.***

3 Ограничения на уровни конфиденциальности для сущностей, функционально ассоциированных с субъектами доступа.

Если $e \in [s]$, ***то верно*** $f_s(s) = f_e(e)$ ***- если сущность функционально ассоциирована с субъектом доступа, то уровень конфиденциальности сущности равен уровню доступа***

субъекта доступа.

4 Ограничения на уровни доступа при управлении субъектами доступа другими субъектами доступа.

Для каждых субъектов доступа $x, y \in S$ ***таких, что*** $y \in control(x)$***, верно равенство*** $f_s(y) = f_s(x)$ ***- если субъект доступа управляется другим субъектом доступа, то их уровни доступа должны быть равны.***

5 Ограничения на информационные потоки.

Для каждых непривилегированного субъекта доступа $x \in N_S$***, субъекта доступа*** $y \in S$ ***и сущности*** $e \in E$ ***таких, что*** $e \in [y]$ ***и*** $(x, e, write_m) \in F$***, верно неравенство*** $f_s(y) <= f_s(x)$ ***- если непривилегированным субъектом доступа реализован информационный поток по памяти к сущности, функционально ассоциированной с другим субъектом доступа, то его уровень доступа не выше уровня доступа непривилегированного субъекта доступа.***

Для каждого информационного потока $(x, y, write_m) \in F$ ***справедливо*** $f_e(x) <= f_e(y)$ ***- разрешены только информационные потоки по памяти, когда сущность-источник имеет уровень конфиденциальности не выше уровня конфиденциальности сущности-приемника.***

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