DOI: 10.15514/ISPRAS-2024-36(3)-5

# О разработке проекта национального стандарта ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке»

*П.Н. Девянин,* ORCID: 0000-0003-2561-794X <*pdevyanin@astralinux.ru*>

*ООО «РусБИТех-Астра»,*
*117105, г. Москва, Варшавское ш., д. 26.*

**Аннотация.** В соответствии с требованиями нормативных документов ФСТЭК России для обеспечения доверия к сертифицированным средствам защиты информации (СЗИ) при реализации ими политик управления доступом должна описываться соответствующая формальная модель. Чтобы стимулировать разработку формальных моделей управления доступом, адекватных условиям функционирования современных СЗИ, в ГОСТ Р 59453.1-2021 «Защита информации. Формальная модель управления доступом. Часть 1. Общие положения» были установлены критерии, которым должно соответствовать описание каждой такой модели, а также дополнительные критерии для случаев, когда СЗИ реализуются конкретные политики: дискреционного, мандатного, ролевого управления доступом или мандатного контроля целостности. Для упрощения процесса описания формальной модели особенно в ситуации, когда СЗИ является сложным системным программным обеспечением, например, операционной системой (ОС) или системой управления базами данных, развития нормативного и методического обеспечения в данной области при участии автора был разработан проект нового национального стандарта ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке», утверждение которого запланировано в 2024 г. В статье анализируются результаты разработки этого проекта, в том числе рекомендуемые в нем этапы описания формальной модели, включая описания состояний и правил перехода из состояний в состояния соответствующего абстрактного автомата, формулирования и осуществления доказательств выполнения условий безопасности, используемые для этого технологии и практические приемы. Кроме того, в статье приводятся примеры апробации изложенных в проекте национального стандарта рекомендаций при переработке мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux (МРОСЛ ДП-модели), используемой в качестве научной основы реализации подсистемы безопасности PARSEC сертифицированной по высшим классам защиты и уровням доверия ОС Astra Linux.

**Ключевые слова:** национальный стандарт; формальная модель управления доступом; рекомендации по разработке; МРОСЛ ДП-модель; Astra Linux.

**Для цитирования:** Девянин П.Н. О разработке проекта национального стандарта ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке», том 36, вып. 3, 2024, стр. 63–82. DOI: 10.15514/ISPRAS–2024–36(3)–5

# On the Development of the Draft Standard GOST R “Information Protection. Formal Access Control Model. Part 3. Recommendations on Development”

*P.N. Devyanin, ORCID: 0000-0003-2561-794X <pdevyanin@astralinux.ru>*

*RusBITech-Astra*

*26, Varshavskoe, Moscow, 117105, Russia*

**Abstract.** Formal models of access control must be described in accordance with the requirements of FSTEC of Russia regulatory documents, in order to ensure trust in certified information security tools when they implement appropriate access control policies. The criterias that the description of each such model must meet were established in GOST R 59453.1-2021 “Information protection. Formal access control model. Part 1. General principles” to stimulate the development of formal access control models that are adequate to the operating conditions of modern information security tools. This standard also specifies additional criteria for cases where specific policies are implemented by information security tools: discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), or mandatory integrity control (MIC). A draft of the new standard GOST R “Information protection. Formal access control model. Part 3. Recommendations on development” was developed with the participation of the author to simplify the process of describing the formal model, which is scheduled for approval in 2024. This new standard is important for the development of regulatory and methodological support in this area. The standard will also be useful in developing a formal model for information security tools that are complex system software, such as an operating system (OS) or a database management system (DBMS). The article analyzes the results of the development of this draft standard, including the stages recommended in it for describing the formal model. Firstly, this is the stage of describing the states of the corresponding abstract automaton. Secondly, this is one of describing the rules for transition from states to states of an abstract automaton. Thirdly, this is the stage of formulating and implementing evidence of the fulfillment of safety conditions, the technologies and practical techniques used for this. In addition, the article provides examples of testing the recommendations set out in the draft standard when reworking the mandatory entity-role model of access and information flows security control in OS of Linux family (MROSL DP-model), which is used as the scientific basis for the implementation of the PARSEC security subsystem of certified according to the highest protection classes and trust levels of OS Astra Linux.

**Keywords:** formal models of access control; MROSL DP-model; role-based access control; mandatory integrity control; operating system; Astra Linux

**For citation:** Devyanin P.N. On the development of the draft standard GOST R “Information protection. Formal access control model. Part 3. Recommendations on development”. Trudy ISP RAN/Proc. ISP RAS, vol. 36, issue 3, 2024. pp. 63-82 (in Russian). DOI: 10.15514/ISPRAS-2024-36(3)-5.

## *1. Введение*

Во многих средствах защиты информации (СЗИ), особенно являющихся многопользовательским распределенным системным программным обеспечением (ПО), например, операционными системами (ОС) или системами управления базами данных (СУБД), реализуются политики управления доступом [1]. Чаще всего, как во многих ОС, это политика дискреционного управления доступом, а также, например, как в ОС семейства Microsoft Windows – еще политика мандатного контроля целостности, реже, как в ОС Astra Linux (операционной системе специального назначения Astra Linux Special Edition) [2, 3] – мандатного управления доступом и мандатного контроля целостности. В СУБД, как правило, используется политика ролевого управления доступом.

Изначально с начала 70-х годов прошлого столетия для научных исследований используемых в СЗИ технологий и механизмов управления доступом разрабатывались соответствующие формальные модели такие, как модели Белла-ЛаПадулы, Харрисона-Руззо-Ульмана, Take-Grant, RBAC и др. [4, 5]. Впоследствии, по мере накопления практик применения формальных моделей при создании, анализе защищенности и обосновании доверия к СЗИ

требования к представлению их описаний стали включаться в нормативные документы и стандарты в области защиты информации.

Первым примером здесь является опубликованный в 1985 г. стандарт TCSEC *(*«Оранжевая книга») [6], в котором в класс защиты B2 было включено требование к описанию формальной модели управления доступом (formal model of the security policy). В дальнейшем аналогичные требования включались в большинство профильных стандартов, в том числе, в ГОСТ Р ИСО/МЭК 15408-3 (ISO/IEC 15408-3) [7], в котором была задана компонента доверия ADV_SPM.1 «Формальная модель политики безопасности». В этой компоненте доверия без раскрытия подробных требований к описанию формальной модели, было указано, что оно должно быть изложено в формальном стиле (с использованием, например, математического языка), должно быть определено понятие «безопасность» и представлено формальное доказательство того, что анализируемое СЗИ (в терминах этого стандарта – объект оценки) не может перейти в небезопасное состояние. Из нормативных документов ФСТЭК России общие требования по разработке модели безопасности СЗИ, реализующего политики управления доступом, в первую очередь были изложены в «Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» [8] и «Методике выявления уязвимостей и недекларированных возможностей в программном обеспечении» [9].

С целью конкретизации, создания лучших условий для выполнения этих требований, нормативного и методического обеспечения этого процесса был разработан и утвержден ГОСТ Р 59453.1-2021 «Защита информации. Формальная модель управления доступом. Часть 1. Общие положения» [1]. В нем изложены критерии, которым должно соответствовать описание формальной модели управления доступом, при этом впервые дано стандартизованное определение самой такой модели как «математического или формализованного (машиночитаемого, пригодного для автоматизированной обработки) описания средства защиты информации и компонентов среды его функционирования, предоставление доступов между которыми регламентируется политиками управления доступом, реализуемыми этим средством защиты информации».

В ГОСТ Р 59453.1-2021 также указано, что описание формальной модели должно быть дано либо на математическом, либо на формализованном (машиночитаемом) языках и включать описание состояний и правил перехода между состояниями абстрактного автомата, соответствующего политикам управления доступом, реализуемым моделируемым СЗИ. Это описание должно быть дано как минимум с использованием терминов: объект доступа (объект, контейнер, сущность), учётная запись пользователя, субъект доступа (субъект), доступ, право доступа, информационный поток. Также должны быть описаны условия безопасности, выполнение которых в абстрактном автомате указывает на реализацию заданных 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.

Каждый раздел ГОСТ Р 59453.1-2021 (посвященный, соответственно, описанию состояний абстрактного автомата, описанию правил его перехода из состояний в состояния и доказательству выполнения условий безопасности во всех его состояниях и при всех переходах из состояний в состояния) разбит на пять частей: первая часть предназначается для изложения критериев, которым должны удовлетворять описания всех формальных моделей управления доступом, а последующие части – для критериев описания моделей для СЗИ, реализующих, соответственно, политики дискреционного, ролевого, мандатного управления доступом и мандатного контроля целостности.

Для стандартизации рекомендаций по верификации с применением инструментальных средств соответствующих критериям ГОСТ Р 59453.1-2021 формальных моделей был разработан и утвержден ГОСТ Р 59453.2-2021 «Защита информации. Формальная модель управления

доступом. Часть 2. Рекомендации по верификации формальной модели управления доступом» [10], в котором были заданы критерии выбора инструментальных средств верификации, даны рекомендации по переводу (при необходимости) описания формальной модели из математического в формализованное (машиночитаемое) описание, а также по автоматическому доказательству непротиворечивости формальной модели и выполнения заданных в ее рамках условий безопасности (условий верификации).

Всем требованиям и критериям перечисленных национальных стандартов соответствует мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в ОС семейства Linux (МРОСЛ ДП-модель) [5], на основе которой «Группой Астра» (в ее состав входит ООО «РусБИТех-Астра») в подсистеме безопасности PARSEC реализуется механизм управления доступом сертифицированной по высшим классам защиты и уровням доверия ОС Astra Linux. Оба стандарта ГОСТ Р 59453.1,2-2021 по сути прошли апробацию на примере описания и верификации этой модели [11, 12].

Вместе с тем разработка формальной модели управления доступом как комплексный многоэтапный процесс может вызывать значительные трудности особенно в случае, когда она необходима для моделирования СЗИ, являющегося системным ПО, ОС или СУБД. Это связано с тем, что для обеспечения адекватности формальной модели такому СЗИ, возможности ее применения в качестве основы для разработки его механизмов защиты, доказательству выполнения им условий безопасности требуется существенная детализация и усложнение формальной модели. В противном случае выводы, полученные при анализе безопасности СЗИ в рамках формальной модели, и она сама могут оказаться бесполезными, далекими от реальных условий функционирования СЗИ.

В этой связи для упрощения процесса разработки формальной модели управления доступом в рамках реализации единой методологии разработки безопасного системного ПО [13] при участии автора настоящей статьи и сотрудников Института системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН) был подготовлен проект нового национального стандарта ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке».

В статье анализируются результаты разработки этого проекта национального стандарта. В ней приводятся примеры апробации изложенных в нем рекомендаций на основе опыта разработки и переработок МРОСЛ ДП-модели [14], многократно выполненных в течение более 10 лет с учетом как развития соответствующей теории, так и изменений в механизмах защиты ОС Astra Linux. Поэтому статья организована следующим образом. В следующем разделе рассматриваются область применения и общие положения проекта национального стандарта. В разделе 3 анализируются изложенные в проекте национального стандарта рекомендации по выбору технологий, инструментальных средств и практических приемов разработки формальной модели управления доступом. В разделе 4 излагаются рекомендации по описанию формальной модели, в том числе состояний и правил перехода между состояниями используемого для моделирования согласно ГОСТ Р 59453.1-2021 абстрактного автомата. Раздел 5 посвящен рекомендациям по описанию и доказательству выполнения условий безопасности, в том числе, при верификации формальной модели управления доступов. Заключение завершает статью, в нем подводятся итоги разработки и апробации анализируемого проекта национально стандарта.

## 2. Область применения и общие положения проекта национального стандарта

В области применения проекта национально стандарта ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке» указывается, что он предназначен для разработчиков СЗИ, реализующих политики управления доступом, а также для органов по сертификации и испытательных лабораторий при проведении сертификации таких СЗИ. При этом в общих положениях проекта определено, что он направлен

на обеспечение соответствия описания разрабатываемой согласно его рекомендациям формальной модели критериям, установленным ГОСТ Р 59453.1-2021.

Для достижения этого в проекте рекомендуются следующие этапы разработки и описания формальной модели:

1. Определение границ моделирования СЗИ;
2. Определение видов политик управления доступом, рассматриваемых при моделировании и реализуемых СЗИ;
3. Выбор технологий, инструментальных средств (при необходимости) и практических приемов разработки формальной модели;
4. Описание формальной модели;
5. Описание и доказательство выполнения условий безопасности, в том числе, при верификации формальной модели.

На этапе 1 рекомендуется зафиксировать назначение формальной модели для существующего или проектируемого СЗИ, т. е. наличие или отсутствие возможности внесения существенных изменений в СЗИ согласно разрабатываемой формальной модели. Это связано с тем, что описание формальной модели для проектируемого СЗИ предоставляет больше возможностей для моделирования, так как подразумевает при этом меньше ограничений, накладываемых неподлежащими изменению режимами функционирования СЗИ. Вместе с тем, моделирование существующего СЗИ позволяет получить больше данных об особенностях его функционирования, и, как следствие более, точно отразить их в формальной модели. Например, с одной стороны при развитии МРОСЛ ДП-модели учитываются особенности функционирования существующей ОС Astra Linux, с другой стороны реализация наследуемого ею от ОС семейства Linux дискреционного управления доступом изначально достаточно проста и не сильно ограничивает возможности для моделирования перспективных мандатного контроля целостности или ролевого управления доступом.

Кроме того, на этапе 1 рекомендуется установить, регламентируют ли политики управления доступом СЗИ предоставление доступов между всеми компонентами среды его функционирования или только их подмножества, а также в целом отразить учитываемые существенные особенности этой среды (наличие сетевой инфраструктуры, применение технологий виртуализации или др.). Хотя моделирование СЗИ, реализующего политики управления доступом для всех компонент среды его функционирования, является более сложным, вместе с тем, оно позволяет при необходимости более точно отразить в описании формальной модели, например, условия возникновения информационных потоков по времени. Кроме того, учет всех особенностей среды функционирования СЗИ может также значительно затруднить моделирование, при этом не оказав существенного влияния на обеспечение соответствия ему описания формальной модели. Например, моделирование управления доступом в ОС 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. Такой подход реализуется в МРОСЛ ДП-модели, где с одной стороны моделируется управление доступом между всеми компонентами ОС Astra Linux, что позволяет анализировать условия создания информационных потоков по времени, с другой стороны, в этой модели сетевая инфраструктура на основе данной ОС пока явно не отражена.

На этапе 2 при определении рассматриваемых при моделировании видов реализуемых СЗИ политик управления доступом рекомендуется использовать политики, определенные в ГОСТ Р 59453.1-2021 (дискреционного, мандатного, ролевого управления доступом и мандатного контроля целостности). При этом учитывать, что необоснованное расширение состава рассматриваемых видов политик может сказаться на сложности моделирования, формулирования и доказательства выполнения условий безопасности, в том числе, при

верификации формальной модели. В этой связи сокращение состава видов политик целесообразно осуществлять за счет возможности выражения политик одних видов политиками других видов. Например, традиционная для ОС семейства Linux политика дискреционного управления доступом в МРОСЛ ДП-модели выражается политикой ролевого управления доступом. При этом используемым в ОС Astra Linux учетным записям пользователей или привилегиям сопоставляются соответствующие им роли.

Рекомендации по выполнению этапов 3-5 разработки и описания формальной модели раскрыты в соответствующих трех разделах проекта национального стандарта, поэтому будут проанализированы в последующих разделах настоящей статьи.

## 3. Рекомендации по выбору технологий, инструментальных средств и практических приемов разработки формальной модели управления доступом

Основной рекомендацией в проекте национального стандарта по выбору языка описания формальной модели управления доступом является использование для этого не менее двух языков: математического и, как минимум, одного из формализованных (машиночитаемых) языков. Это обусловлено тем, что применение математического описания формальной модели [5] всегда допускает полную независимую от ее разработчика проверку корректности этого описания, заданных в формальной модели условий безопасности, а также всех выполненных в модели доказательств. Они приводятся непосредственно в описании формальной модели, что предоставляет возможность объективного анализа их корректности любым специалистом, знакомым с языком математики.

Использование формализованного описания позволяет с применением инструментальных средств, реализующих формальные методы, поддерживающие выбранный язык этого описания, осуществить автоматическую верификацию формальной модели, доказательство ее непротиворечивости [11]. Также в этом случае, 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.

К примеру, МРОСЛ ДП-модель описывается на математическом языке и на языке формального метода Event-B [12]. При этом с использованием второго описания эта модель верифицируется с применением инструментальных средств дедуктивно (с помощью инструментального средства Rodin) и по методу проверки моделей (с помощью инструментального средства ProB).

Приступая к разработке формальной модели управления доступом, рекомендуется проанализировать существующие формальные модели, в первую очередь соответствующие актуальным для моделируемого СЗИ политикам управления доступом и среде его функционирования (ОС, СУБД или др.). По результатам такого анализа целесообразно выбрать базовую формальную модель, на основе которой осуществлять дальнейшую разработку. Также могут быть отобраны другие модели, элементы которых отсутствуют в базовой модели, и которые целесообразно включить в разрабатываемую формальную модель как существенные для моделирования СЗИ. При этом следует отметить недостатки базовой формальной модели, не позволяющие непосредственно ее использовать, и которые в итоге необходимо устранить.

Например, существенным для многих СЗИ является использование иерархии объектов доступа (сущностей, файлов, каталогов), привилегированных и непривилегированных учетных записей пользователей, привилегированных и непривилегированных субъектов. Многие формальные модели, известные как классические (например, модели Белла-ЛаПадулы, Take-Grant, RBAC [4, 5]), не моделируют перечисленные свойства и элементы СЗИ. Также эти модели не позволяют моделировать информационные потоки (скрытые каналы) по времени. Вместе с тем существуют формальные модели (например, МРОСЛ ДП-модель), в которых эти свойства моделируются.

В проекте национального стандарта рекомендуются следующие технологии и практические приемы разработки формальной модели управления доступом:

- Поэтапное усложнение формальной модели;
- Объединение нескольких формальных моделей на основе базовой формальной модели;
- Разработка иерархического представления формальной модели;
- Разработка на основе базовой формальной модели сокращенной (редуцированной) формальной модели;
- Разработка отдельных формальных моделей для компонентов СЗИ.

При поэтапном усложнении формальной модели на каждом этапе, начиная с базовой формальной модели, свойства СЗИ 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. Это рекомендуется в связи с тем, что разрабатываемая формальная модель может быть достаточно сложной, поэтому допущенные при ее описании неточности или противоречия могут быть выявлены только на завершающем этапе ее разработки. При этом их устранение может потребовать полной переработки формальной модели. Использование поэтапного усложнения формальной модели позволяет своевременно выявлять большинство неточностей или противоречий в первую очередь за счет доказательства выполнения условий безопасности и верификации, соответствующих каждому этапу разработки ее представления. Кроме того, каждый этап разработки формальной модели может соответствовать описанию в ее рамках только некоторых свойств СЗИ или среды его функционирования, что также упрощает моделирование. Например, можно сначала моделировать только информационные потоки по памяти между субъектами и объектами доступа СЗИ, и только после завершения этого включить в формальную модель элементы, позволяющие анализировать информационные потоки по времени.

Объединение нескольких формальных моделей управления доступом на основе базовой формальной модели рекомендуется при необходимости заимствования их элементов особенном в случае моделирования СЗИ, реализующего несколько политик управления доступом, или состоящего из нескольких систем (например, ОС и СУБД), 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 СЗИ.

Например, при моделировании мандатного управления доступом с применением элементов моделей ролевого управления доступом назначаемые ролям права доступа к объектам доступа могут быть использованы для создания информационных потоков по времени от объектов доступа с большим уровнем конфиденциальности к объектам доступа с меньшим уровнем конфиденциальности [5], что нарушает требования первой политики. Для предотвращения возможности возникновения таких скрытых каналов может быть использовано назначение ролям уровней конфиденциальности и предоставление их субъектам в качестве текущих (в том числе возможности изменения ими прав доступа ролей) только в случае, когда уровень доступа соответствующего субъекта не ниже уровня конфиденциальности соответствующей роли. Именно такой подход применен в МРОСЛ ДП-модели.

При разработке иерархического представления формальной модели рекомендуется описывать ее по слоям (уровням), при этом каждый нижний слой 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. Использование такого представления существенно упрощает разработку формальной модели особенно в случае, когда моделируемое СЗИ реализует несколько политик управления доступом, или оно состоит из нескольких систем (например, ОС и СУБД). Тогда каждой политике управления доступом или каждой системе может быть сопоставлен отдельный слой или слои иерархического представления формальной модели. При этом доказательство выполнения условий безопасности и верификация формальной модели может быть осуществлено последовательно по слоям. Выбор последовательности слоев при описании формальной модели в ее иерархическом представлении может быть осуществлен, исходя из непосредственной технической реализации моделируемого СЗИ (например, слой, соответствующий ОС будет ниже слоя, соответствующего СУБД).

Этот прием многократно апробирован при описании МРОСЛ ДП-модели, которое на математическом и на формализованном языках имеет иерархическое представление, состоящее из восьми уровней – четырех уровней для моделирования управления доступом непосредственно в ОС: ролевого управления доступом (для штатного у ОС семейства Linux дискреционного управления доступом), мандатного контроля целостности, мандатного управления доступом с информационными потоками по памяти, мандатного управления доступом с информационными потоками по времени, и четырех уровней для решения аналогичной задачи в штатной для ОС СУБД PostgreSQL. Это обеспечивает согласованность механизмов управления доступом в ОС и СУБД, а также соответствует подходу по реализации модели непосредственно в программном коде подсистемы безопасности PARSEC ОС Astra Linux.

Разработка на основе базовой формальной модели сокращенной (редуцированной) формальной модели рекомендуется, когда базовая формальная модель включает некоторые элементы, избыточные для описания моделируемого СЗИ. При этом в редуцированную модель включают подмножество элементов базовой формальной модели или задают ограничения, обеспечивающие возможность применения инструментальных средств автоматической верификации модели. Это может потребоваться, когда из-за большей сложности затруднена верификация базовой формальной модели (например, из-за проблемы «комбинаторного взрыва» может стать невозможной верификация по методу проверки моделей – model checking). Например, может быть ограничен состав элементов начального состояния описываемого в рамках формальной модели абстрактного автомата.

При разработке отдельных формальных моделей для компонентов СЗИ рекомендуется дать обоснование отсутствия влияния каждого компонента на реализацию политик безопасности другими компонентами. Например, в случае моделирования СЗИ, 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 СЗИ (например, функционирующих на сервере или на рабочей станции) при наличии у них существенных отличий могут быть разработаны отдельные формальные модели управления доступом.

## *4. Рекомендации по описанию формальной модели управления доступом*

Непосредственное описание формальной модели управления доступом в проекте национального стандарта рекомендуется начинать с состояний абстрактного автомата, которые должны включать перечисленные в ГОСТ Р 59453.1-2021 множества: учетных записей пользователей, субъектов доступа (субъектов), объектов доступа, реализуемых доступов субъектов к объектам доступа, реализуемых прав доступа субъектов к объектам или субъектам, информационных потоков, а также описания условий внутренней и взаимной корректности (согласованности) этих множеств и заданных на них функций (отношений).

При этом рекомендуется учитывать, что во множество учетных записей пользователей целесообразно включить не только элементы, соответствущие явно реализованным в моделируемом СЗИ, но также учетные записи системных пользователей (псевдопользователей, от имени которых, например, функционируют некоторые процессы ядра ОС), что может позволить более точно смоделировать режимы функционирования СЗИ. Например, при реализации в СУБД PostgreSQL политики ролевого управления доступом учетные записи пользователей могут не задаваться вообще. Вместо них используются роли (называемые ролями входа), с получения которых начинается сеанс работы в такой системе. Этим ролям при описании формальной модели могут быть сопоставлены одноименные им элементы множества учетных записей пользователей.

Элементы множества субъектов рекомендуется ставить в соответствие каждому субъекту среды функционирования СЗИ. При этом в некоторых случаях для упрощения описания формальной модели нескольким таким компонентам СЗИ может ставиться в соответствие один субъект, например, когда в ОС в одной сессии от имени одной учетной записи пользователя функционируют обладающие одинаковыми правами доступа процессы.

В свою очередь элементы множества объектов доступа, как правило, ставятся в соответствие каждому такому компоненту среды функционирования СЗИ. На этом множестве задается соответствующее используемому в СЗИ отношение иерархии. При этом в случае ОС или СУБД, которые могут включать миллионы объектов доступа, может потребоваться сокращение числа элементов множества объектов доступа. Например, для СУБД это может быть сделано моделированием управления доступом только до таблиц базы данных. Тогда права доступа и доступы субъектов к записям таблиц могут быть смоделированы как права доступа и доступы к самим таблицам (например, доступ субъекта на чтение к записи таблицы может при моделировании описываться как доступ на чтение к этой таблице целиком). Отношение иерархии на множестве объектов доступа описывается в соответствии с тем, как оно реализовано в моделируемом СЗИ. Например, заданное в МРОСЛ ДП-модели отношение иерархии объектов доступа (сущностей) позволяет описывать штатные для ОС семейства Linux «жесткие» ссылки (hard link), когда некоторый соответствующий файлу объект доступа может одновременно непосредственно подчиняться в иерархии нескольким объектам доступа, соответствующим каталогам (контейнерам).

Осуществляя описание множества реализуемых доступов субъектов к объектам доступа, рекомендуется учитывать, что для большинства моделируемых СЗИ и реализуемых ими политик управления доступом достаточно использовать только два вида доступа: на чтение и на запись. В то же время при описании множества реализуемых прав доступа субъектов к объектам доступа учитывать возможное многообразие способов задания таких прав в СЗИ. При этом эти права доступа могут быть универсальными для всех субъектов и объектов доступа или зависеть от их конкретных экземпляров. Так в ОС такие права доступа к файлам или каталогам в большинстве случаев можно рассматривать как универсальные (например, на чтение, запись, выполнение, владение). Вместе с тем в СУБД называемые привилегиями права доступа часто существенно зависят от назначения конкретных объектов доступа (например, к таблицам может назначаться широкий спектр привилегий: SELECT, INSERT, UPDATE, DELETE, TRUNCATE, а к функциям – только привилегия EXECUTE), что необходимо учитывать при моделировании. Кроме того, в СУБД 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.

При моделировании СЗИ, состоящего из нескольких систем (например, ОС и СУБД), самостоятельно реализующих политики управления доступом, рекомендуется задать отношение соответствия между правами доступа, используемыми в каждой из систем, что удобно для анализа информационных потоков, возникающих между их субъектами и

объектами доступа. Например, отношение соответствия между следующими привилегиями СУБД и правами доступа в ОС может быть задано так:

- 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) и $write_r$ (право доступа на запись).

Для описания множества информационных потоков рекомендуется включить в него информационные потоки по памяти, а включение информационных потоков по времени целесообразно при моделировании СЗИ, реализующего политику мандатного управления доступом. В таких СЗИ является нарушением условий безопасности 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 и поток по времени. При этом для СЗИ, 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.

Для задания условий внутренней и взаимной корректности (согласованности) используемых для описания состояний абстрактного автомата множеств, функций (отношений) целесообразно их явно формулировать, основываясь на логике применения этих функций и отношений, исходя из необходимости обеспечения их соответствия компонентам, свойствам моделируемого СЗИ и реализуемых им политик управления доступом. Для сокращения числа неточностей или противоречий проверку выполнения этих условий рекомендуется осуществлять сразу при появлении такой возможности, в том числе после каждого этапа разработки формальной модели или после описания каждого слоя иерархического представления формальной модели. Кроме того, эти условия желательно использовать при формализованном описании и автоматической верификации формальной модели.

Примерами условий внутренней и взаимной корректности множеств, функций (отношений), используемых для описания состояний абстрактного автомата, являются:

- В иерархии объектов доступа (сущностей) только являющиеся объектами доступа контейнеры могут содержать другие объекты доступа;
- Субъекты могут иметь к друг 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 не превосходит уровня доступа учетной записи пользователя, от имени которой он функционирует.

После описания состояний абстрактного автомата в рамках формальной модели управления доступом рекомендуется описать правила его перехода из состояний в состояния (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 СЗИ. При этом желательно, чтобы с каждой непосредственно связанной с реализацией политик управления доступом функцией (системным вызовом, хранимой процедурой, событием или др.) СЗИ было сопоставлено правило (или правила) 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 СЗИ, 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 управления другими субъектами. Также для каждого правила в его параметрах, условиях и результатах применения следует указывать субъекта (или субъектов), который может являться инициатором его выполнения.

Порядок сопоставления функций СЗИ и правил перехода из состояний в состояния абстрактного автомата зависит от свойств этого СЗИ, удобства при моделировании и применяемых для этого технологий. Например, системному вызову в ОС, осуществляющему 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 созданий файлов, каталогов, сокетов или других сущностей. Если состав и описание де-юре правил часто сильно зависят от моделируемого СЗИ, то состав и описание де-факто правил достаточно универсальны (в качестве их примера удобно использовать де-факто правила из расширенной модели Take-Grant или МРОСЛ ДП-модели). Явное задание в каждом де-юре и де-факто правиле субъекта, как инициатора его выполнения, соответствует тому, что только субъекты (например, процессы), как активные компоненты среды функционирования СЗИ, могут инициировать выполнение каких-либо его функций.

Кроме того, при описании состояний и правил перехода из состояний в состояния абстрактного автомата рекомендуется учитывать перспективы дальнейшего формулирования условий безопасности, математического или формального (при верификации формальной модели с применением инструментальных средств) доказательства их выполнения. Для этого при наличии возможности правила перехода, в которых только добавляются новые элементы состояний (монотонными правилами), описывать отдельно от правил, в которых эти элементы удаляются (немонотонные правила). Иногда, как, например, в модели Take-Grant, это упрощает математическое доказательство выполнения условий безопасности (особенно в случае, когда моделируемое СЗИ реализует дискреционное управление доступом) [4, 5].

Также в условиях и результатах применения де-юре правил целесообразно избегать использования информационных потоков или управления одними субъектами другими субъектами. Наоборот, в результатах применения де-факто правил не следует вносить изменения в элементы описания состояний абстрактного автомата, которые непосредственно реализуются в СЗИ. Если 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, и которые могут повлиять на успешность использования этих средств для ее верификации. Например, поскольку большинство инструментальных средств автоматической верификации по методу проверки моделей (model checking) чувствительны к числу элементов состояний описываемого в рамках формальной модели абстрактного автомата, то учесть такое ограничение часто возможно за счет разработки сокращенной (редуцированной) формальной

модели или (при наличии такой возможности) отдельных формальных моделей для каждого компонента СЗИ.

Кроме общих рекомендаций для каждой из рассмотренных в ГОСТ Р 59453.1-2021 политик управления доступом в проекте национального стандарта даются дополнительные рекомендации по описанию соответствующей им формальной модели.

Если моделируемое СЗИ реализует политику дискреционного управления доступом, то при разработке формальной модели дополнительно рекомендуется выбрать способ описания матрицы доступов, наиболее соответствующий тому, как она в нем непосредственно задается. Например, чаще всего в СЗИ она задается назначением каждому объекту доступа прав доступа к нему субъектам либо с помощью маски бит (например, как в ОС семейства Linux), либо с помощью списков контроля доступа (например, ACL как в ОС семейства Windows). Применение способов описания матрицы доступов, не связанных с тем, как она задается в СЗИ, 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 СЗИ.

Если моделируемое СЗИ реализует политику ролевого управления доступом, то при разработке формальной модели дополнительно рекомендуется:

- В множестве ролей задать подмножество административных ролей, позволяющих обладающим ими в качестве текущих субъектам 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). Также если в моделируемом СЗИ имеются административные роли, которые либо не могут непосредственно создаваться, удаляться, изменять в процессе его функционирования свои параметры (например, роль postgres в СУБД PostgreSQL), либо такое предположение допустимо при моделировании, то для упрощения описания формальной модели (особенно правил перехода из состояний в состояния абстрактного автомата) в 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 СЗИ политик управления доступом. Например, если СЗИ также реализует политику мандатного управления доступом, то имена ролей могут использоваться для создания информационных потоков (скрытых каналов) по времени, и их целесообразно включить в описание формальной модели;

- Если СЗИ 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 СЗИ. Например, в МРОСЛ ДП-модели множества ролей для ОС и СУБД заданы отдельно.

Если моделируемое СЗИ реализует политику мандатного контроля целостности, то при разработке формальной модели дополнительно рекомендуется:

- Учесть при задании множеств учетных записей привилегированных и непривилегированных пользователей важность корректного включения в них каждой

конкретной учетной записи пользователя, исходя из наличия или отсутствия у него полномочий по управлению или администрированию моделируемого СЗИ;

- Задать привилегированным учетным записям пользователей и привилегированным субъектам максимальный в решетке уровней целостности уровень целостности, а непривилегированным учетным записям пользователей и непривилегированным субъектам уровни целостности меньше максимального, например, минимальный уровень целостности;

- Включить в описание формальной модели множество информационных потоков по памяти, а также предназначенные для использования таких информационных потоков де-факто правила, поскольку такие информационные потоки существенны для описания условий безопасности при моделировании СЗИ, реализующих политику мандатного контроля целостности;

- Задать для каждого субъекта множество функционально ассоциированных с ним объектов доступа, что является существенным для описания условий безопасности, связанных с наличием возможности одних субъектов (особенно непривилегированных) получать управление другими субъектами (особенно привилегированными). Например, в ОС у каждого субъекта (процесса) есть хотя бы один функционально ассоциированный с ним объект доступа (исполняемый файл, из которого этот процесс был активизирован). При этом такими объектами доступа могут быть также файлы динамических библиотек, конфигурационные файлы, сегменты оперативной памяти и др.;

- Задать (при необходимости) подмножество привилегированных субъектов, доступы которых к объектам доступа не могут быть использованы для создания информационных потоков по памяти от непривилегированных субъектов к объектам доступа, функционально ассоциированным с привилегированными субъектами. Это рекомендуется в связи с тем, что в большинстве СЗИ существуют объекты доступа (например, сокеты в ОС) через которые могут осуществлять обмен данными привилегированные и непривилегированные субъекты. При этом такие объекты доступа часто имеют минимальный уровень целостности, в результате к ним могут получать доступы на запись непривилегированные субъекты, а на чтение – привилегированные субъекты. Если непосредственно описать это в разрабатываемой формальной модели, то возможна ситуация, когда с участием привилегированных субъектов возможно создание информационных потоков по памяти от непривилегированных субъектов к объектам доступа, функционально ассоциированным с привилегированными субъектами, что будет приводить к нарушению условий безопасности (например, получению управления непривилегированными субъектами привилегированными субъектами). Для предотвращения этого в СЗИ доступы на чтение привилегированных субъектов к объектам доступа, через которые ими осуществляется обмен данными с непривилегированными субъектами, реализуется таким образом, чтобы эти доступы (например, через интерфейсы сокетов ОС) не могли использоваться для создания рассматриваемых информационных потоков по памяти. Такой подход применен в МРОСЛ ДП-модели путем задания в ней подмножества привилегированных субъектов, корректных относительно объектов доступа и субъектов;

- Если СЗИ состоит из нескольких систем, самостоятельно реализующих политику мандатного контроля целостности, задать при разработке формальной модели множество информационных потоков по памяти и единые для всех этих систем решетку уровней целостности, а также функции (отношения), используемые для

задания уровней целостности учетных записей пользователей, субъектов и объектов доступа. В таких СЗИ (например, состоящих из ОС и СУБД) доступы субъектов к объектам доступа одной системы могут быть использованы для нарушения условий безопасности в другой системе. Например, непосредственные доступы процессов ОС к ее файлам, в которых содержатся записи СУБД. Поэтому при моделировании таких СЗИ желательно задание единых для всех систем решетки уровней целостности, функций (отношений), используемых для задания соответствующих уровней целостности, множества информационных потоков по памяти, а также единых правил перехода из состояний в состояния абстрактного автомата;

- Использовать решетку уровней целостности, содержащую меньшее число элементов, чем реализовано в моделируемом СЗИ, для упрощения описания формальной модели, в том числе когда разрабатывается сокращенная (редуцированная) формальная модель. Это связано с тем, что для описания большинства условий безопасности при моделировании СЗИ, реализующих политику мандатного контроля целостности, может оказаться достаточно всего двух уровней целостности, например, «высокая целостность» (для привилегированных учетных записей пользователей, функционирующих от их имени субъектов, 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 СЗИ, может быть полезным при верификации формальной модели по методу проверки моделей (model checking), реализующие который инструментальные средства чувствительны к числу элементов состояний описываемого в ее рамках абстрактного автомата.

Если моделируемое СЗИ реализует политику мандатного управления доступом, то при разработке формальной модели дополнительно рекомендуется:

- Включить в описание разрабатываемой формальной модели множество информационных потоков по памяти и по времени, а также предназначенные для использования таких информационных потоков де-факто правила перехода из состояний в состояния абстрактного автомата, поскольку такие информационные потоки существенны для описания условий безопасности при моделировании СЗИ, реализующих политику мандатного управления доступом;

- Использовать иерархическое представление формальной модели, состоящее, как минимум, из двух слоев, на первом из которых при описании формальной модели задать только множество информационных потоков по памяти, на втором слое – множество информационных потоков по памяти и по времени. Это рекомендуется поскольку в отличие от информационных потоков по памяти описание информационных потоков по времени, а также предназначенных для их использования де-факто правил часто является более сложной задачей. Поэтому для упрощения разработки формальной модели, сокращения допущенных при ее описании неточностей или противоречий целесообразно использование ее такого иерархического представления;

- Задать при разработке формальной модели СЗИ, состоящего из нескольких систем, самостоятельно реализующих политику мандатного управления доступом, единые для всех этих систем решетку уровней конфиденциальности, функции (отношения), используемые для задания уровней доступа учетных записей пользователей и субъектов, уровней конфиденциальности объектов доступа, а также множество информационных потоков по памяти и по времени. В таких СЗИ аналогично тем, которые реализуют политику мандатного контроля целостности, доступы субъектов к

объектам доступа одной системы могут быть использованы для нарушения условий безопасности в другой системе. Особенно такие доступы могут быть использованы для создания запрещенных этими условиями безопасности информационных потоков по времени между объектами доступа (например, от объектов доступа с большим уровнем конфиденциальности к объектам доступа с меньшим уровнем конфиденциальности) систем, из которых состоит СЗИ. Кроме того, при моделировании таких СЗИ при наличии возможности целесообразно задание единых правил перехода из состояний в состояния абстрактного автомата;

- Использовать решетку уровней конфиденциальности, содержащую меньшее число элементов, чем реализовано в моделируемом СЗИ, для упрощения описания формальной модели, в том числе, когда разрабатывается сокращенная (редуцированная) формальная модель. Для описания большинства условий безопасности при моделировании СЗИ, реализующих политику мандатного управления доступом (аналогично политике мандатного контроля целостности), может оказаться достаточно всего двух уровней конфиденциальности (например, «высокая конфиденциальность» и «низкая конфиденциальность»), что также может быть полезным при верификации формальной модели по методу проверки моделей.

Примером реализации приведенных в проекте национального стандарта рекомендаций является МРОСЛ ДП-модель, в которой определены 35 де-юре правил преобразования состояний, предназначенных для формального описания (спецификации) основных функций подсистемы безопасности PARSEC ОС Astra Linux:

- Создание, удаление, переименование, перемещение, получение или изменение параметров учетных записей пользователей, субъектов, сущностей или «жестких» ссылок на них, ролей, запрещающих ролей, административных ролей;
- Получение доступов субъектов к сущностям, административных доступов к ролям, запрещающим ролям или административным ролям;
- Изменение прав доступа ролей, запрещающих ролей или административных ролей к сущностям, субъектам, ролям, запрещающим ролям или административным ролям;
- Изменение иерархий сущностей, ролей, запрещающих ролей или административных ролей;
- Управление множествами запрещающих ролей для ролей и административных ролей;
- Применение авторизованной роли или административной роли от имени учетной записи пользователя;
- Изменение уровней целостности, конфиденциальности и доступа учетных записей пользователей, сущностей, ролей, запрещающих ролей или административных ролей;
- Задание объектов, параметрически ассоциированных с учетными записями пользователей, ролями или административными ролями.

Также в МРОСЛ ДП-модели определены 10 де-факто правил преобразования состояний, которые предназначены для задания условий создания информационных потоков по памяти и по времени или получения одним субъектом возможности управления другим субъектом.

## *5. Рекомендации по описанию и доказательству выполнения условий безопасности*

Согласно ГОСТ Р 59453.1-2021 при разработке формальной модели управления доступом должны быть описаны условия безопасности состояний абстрактного автомата и условия безопасности его переходов из состояний в состояния, для чего должны быть использованы определенные в нем политики управления доступом. В свою очередь, в проекте национального

стандарта ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке» рекомендуется конкретизировать эти политики с учетом деталей их реализации в моделируемом СЗИ. Например, согласно определению политики мандатного управления доступом при получении доступа на запись к объекту доступа уровень доступа субъекта должен быть не выше уровня конфиденциальности объекта доступа. Вместе с тем в ОС семейства Linux существуют объекты доступа (например, файлы /dev/null и /dev/zero), доступ на чтение и запись к которым необходимо разрешить субъектам с любым уровнем доступа. Для учета этого при описании условий безопасности целесообразно для таких объектов доступа сделать соответствующее исключение.

Кроме того, рекомендуется 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). Это объясняется тем, что существуют формальные модели, проверка заданных в которых условий безопасности является в общем случае алгоритмически неразрешимой задачей (например, предназначенная для моделирования СЗИ, реализующих политику дискреционного управления доступом, модель Харрисона-Руззо-Ульмана) или, наоборот, алгоритмически разрешимой задачей (например, предназначенная для моделирования СЗИ, реализующих политику мандатного управления доступом, модель Белла-ЛаПадулы) [4, 5].

Также кроме условий безопасности состояний абстрактного автомата целесообразно определить дополнительные условия безопасности его начального состояния (или начальных состояний), стремясь к упрощению дальнейшего математического (формального) доказательства выполнения условий безопасности. Например, такими дополнительными условиями могут быть требования к отсутствию в начальном состоянии информационных потоков или доступов субъектов к объектам доступа.

При описании условий безопасности, исходя из режимов функционирования моделируемого СЗИ и реализуемых им политик управления доступом, рекомендуется накладывать ограничения на состав и параметры используемых при этом правил перехода между состояниями абстрактного автомата. К примеру, при моделировании СЗИ, 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. Такое ограничение может соответствовать режиму функционирования СЗИ, когда привилегированные субъекты выполнили свои функции по его администрированию, и в нем функционируют только непривилегированные субъекты.

Аналогично рекомендациям по описанию формальной модели для каждой из рассмотренных в ГОСТ Р 59453.1-2021 политик управления доступом в проекте национального стандарта даются дополнительные рекомендации по описанию и осуществлению доказательства выполнения условий безопасности.

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

Если моделируемое СЗИ реализует политику ролевого управления доступом, то при описании условий безопасности дополнительно рекомендуется изложить условия, в которых накладываются следующие ограничения:

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

- На обладание субъектами, не осуществляющими управление или администрирование моделируемым СЗИ, административными ролями.

Если моделируемое СЗИ реализует политику мандатного контроля целостности, то при описании условий безопасности дополнительно рекомендуется задать следующие ограничения:

- На уровень целостности каждого субъекта, 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, который должен быть не ниже уровня целостности этого субъекта;
- На возможность управления субъектом другим субъектом только в случае, когда уровень целостности первого субъекта не ниже уровня целостности второго субъекта;
- На информационные потоки по памяти, из которых должны быть запрещены такие информационные потоки от любого субъекта к объекту доступа, функционально ассоциированному с каким-либо субъектом, когда уровень целостности первого субъекта меньше или не сравним с уровнем целостности этого объекта доступа.

Если моделируемое СЗИ реализует политику мандатного управления доступом, то при описании условий безопасности дополнительно рекомендуется задать следующие ограничения:

- На уровень доступа каждого субъекта, 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, который либо должен быть равен уровню доступа этого субъекта, либо, если в моделируемом СЗИ реализуется политика мандатного контроля целостности, то уровень целостности этого объекта доступа равен максимальному уровню целостности;
- На возможность управления субъектом другим субъектом только в случае, когда уровень доступа первого субъекта равен уровню доступа второго субъекта;
- 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.

Для демонстрации взаимосвязи условий безопасности с режимами функционирования моделируемого СЗИ рекомендуется путем задания соответствующих ему конкретных значений элементов описания состояний абстрактного автомата (множествам учетных записей пользователей, субъектов, объектов доступа, прав доступа, доступов, 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 СЗИ, используемых для реализации им политик управления доступом. Если применяемые для верификации формальной модели 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 СЗИ, происходящим в результате соответствующих таким правилам действий над ним (например, вызовам системных интерфейсов в ОС или запросам, вызовам функций или триггеров в СУБД).

Например, при верификации формальной модели 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 СЗИ удобно проверять соответствие этих траекторий результатам выполнения последовательностей моделируемых правилами переходов между состояниями абстрактного автомата действий в СЗИ.

При доказательстве выполнения условий безопасности в случае, когда для описания формальной модели 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.

При доказательстве выполнения условий безопасности в случае, когда для описания формальной модели управления доступом используется формализованный (машиночитаемый) язык, следует руководствоваться рекомендациями ГОСТ Р 59453.2-2021 [10], осуществляя доказательство автоматически, а при невозможности такого доказательства, выполняя интерактивное доказательство. При этом целесообразно использовать различные технологии верификации формальной модели управления доступом (например, дедуктивную верификацию и верификацию по методу проверки моделей) [12]. Это позволяет своевременно выявлять большее число ошибок или дефектов, допущенных при описании формальной модели.

Если при разработке формальной модели в соответствии с рекомендациями проекта национального стандарта осуществляется поэтапное усложнение ее описания, используется ее иерархическое представление или формируются отдельные формальные модели, то целесообразно осуществлять доказательство выполнения условий безопасности, соответственно, после окончания каждого этапа описания формальной модели, разработки каждого слоя ее иерархического представления или каждой отдельной формальной модели.

В случае, когда для каждого из компонентов моделируемого СЗИ разрабатываются отдельные формальные модели, рекомендуется (при наличии такой возможности) осуществить доказательство отсутствия влияния каждого из компонентов на выполнение условий безопасности в других компонентах.

Большинство рассмотренных рекомендаций были многократно применены при разработке и переработке МРОСЛ ДП-модели [14]. Так в этой модели в ее математическом и формализованном описаниях приводятся определение безопасного начального состояния системы (состояния, в котором отсутствуют запрещенные информационные потоки по памяти или по времени, управление субъектами друг другом, а информационные потоки по памяти или доступы к сущностям, параметрически или функционально ассоциированным с субъектами, не нарушают правил мандатного контроля целостности) и определения трех смыслов нарушения безопасности системы:

- В смысле мандатного контроля целостности, позволяющее недоверенному субъекту с низким уровнем целостности захватить управление (де-факто владение) субъектом с более высоким уровнем целостности;
- В смысле Белла-ЛаПадулы, результатом которого является создание запрещенного информационного потока по памяти «сверху-вниз»;

- В смысле контроля информационных потоков по времени – создание запрещенного информационного потока по времени «сверху-вниз» между сущностями.

С использованием этих определений в модели сформулированы и обоснованы математически (с применением доказательства от противного индукцией по длине последовательности состояний абстрактного автомата) и с применением инструментального средства дедуктивной верификации Rodin достаточные условия безопасности системы во всех трех смыслах, которые являются алгоритмически проверяемыми.

Кроме того, специалистами ИСП РАН и «Группы Астра» разрабатывается программный комплекс, позволяющий собирать обрабатываемые подсистемой безопасности PARSEC ОС Astra Linux трассы системных вызовов и с применением инструментального средства ProB осуществлять проверку их соответствия последовательностям правил переходов между состояниями абстрактного автомата, заданного в рамках МРОСЛ ДП-модели.

## *6. Заключение*

В настоящей статье изложены и проанализированы основные рекомендации являющегося продолжением ГОСТ Р 59453.1,2-2021 разработанного при участии автора проекта нового национального стандарта ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке». Для этого рассмотрены его область применения и общие положения, рекомендации по выбору технологий, инструментальных средств и практических приемов разработки и описания формальной модели управления доступом, включая описания состояний и правил перехода между состояниями используемого для моделирования абстрактного автомата, доказательству выполнения условий безопасности, в том числе, при верификации формальной модели.

Рекомендации проекта национально стандарта были подготовлены с учетом опыта разработки и переработки МРОСЛ ДП-модели, являющейся научной основой реализации подсистемы безопасности PARSEC сертифицированной по высшим классам защиты и уровням доверия ОС Astra Linux. Поэтому анализируемые в статье рекомендации сопровождались примерами их использования при описании этой формальной модели.

Таким образом, настоящая статья по сути является этапом апробации проекта национального стандарта. В 2024 г. планируется завершить его общественное обсуждение и утверждение, после чего он может быть полезен специалистам по защите информации, осуществляющим разработку в первую очередь сертифицированных СЗИ при описании соответствующих им формальных моделей управления доступом.

## Список литературы / References

[1]. ГОСТ Р 59453.1-2021 «Защита информации. Формальная модель управления доступом. Часть 1. Общие положения». М.: Стандартинформ. 16 с. / GOST R 59453.1-2021 «Information protection. Formal access control model. Part 1. General principles», 2021 (in Russian).

[2]. Операционная система специального назначения Astra Linux Special Edition. Доступно по ссылке: https://astragroup.ru/software-services/os/, 03.05.2024. / Astra Linux Special Edition operating system. Available at: https://astragroup.ru/software-services/os/, accessed 03.05.2024.

[3]. Девянин П.Н., Тележников В.Ю., Третьяков С.В. Основы безопасности операционной системы Astra Linux Special Edition. Управление доступом. Учебное пособие. М., Горячая линия – Телеком, 2022, 148 стр. / Devyanin P.N., Telezhnikov V.Y., Tret'yakov S.V. Astra Linux Special Edition security basics. Access control. Hotline-Telecom, 2022, 148 p. (in Russian).

[4]. Bishop M. Computer Security: Art and Science, 2nd edition. Pearson Education Inc., 2018, 1440 p.

[5]. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 3-е изд., перераб. и доп. М.: Горячая линия – Телеком, 2020. 352 с.: ил. / P.N. Devyanin. Security models of computer systems. Control for access and information flows. Hotline-Telecom, 2013, 338 p. (in Russian).

[6]. Trusted Computer System Evaluation Criteria / US Department Of Defense, 1985. CSC-STD-001-83.

[7]. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности». М.: Стандартинформ. 150 с. / GOST R ISO/IEC 15408-3-2013 «Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance components», 2013 (in Russian).

[8]. Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 2 июня 2020 г. N 76. Доступно по ссылке: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-2-iyunya-2020-g-n-76, 03.05.2024 / Excerpts from Requirements for information security approved by FSTEK Russia order #76 of 2nd June 2020. Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-2-iyunya-2020-g-n-76, accessed 03.05.2024. (in Russian).

[9]. Информационное сообщение ФСТЭК России от 10.02.2021 № 240/24/647. Доступно по ссылке: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-10-fevralya-2021-g-n-240-24-647, 03.05.2024 / Informational message of FSTEK Russia of 10th February 2021 #240/24/647. Available at: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-10-fevralya-2021-g-n-240-24-647, accessed 03.05.2024. (in Russian).

[10]. ГОСТ Р 59453.2-2021 «Защита информации. Формальная модель управления доступом. Часть 2. Рекомендации по верификация формальной модели управления доступом». М.: Стандартинформ. 12 с./ GOST R 59453.2-2021 «Information protection. Formal access control model. Part 2. Recommendations on verification of formal access control model», 2021 (in Russian).

[11]. Девянин П.Н., Ефремов Д.В., Кулямин В.В., Петренко А.К., Хорошилов А.В., Щепетков И.В. Моделирование и верификация политик безопасности управления доступом в операционных системах. М.: Горячая линия – Телеком, 2019. 214 с.: ил./ P.N. Devyanin, D.V. Efremov, V.V. Kuliamin, A.K. Petrenko, A.V. Khoroshilov. Modeling and verification of access control access policies in operating systems. Hotline-Telecom, 2019, 214 p. (in Russian).

[12]. Девянин П.Н., Леонова М.А. Приемы по доработке описания модели управления доступом ОССН Astra Linux Special Edition на формализованном языке метода Event-B для обеспечения ее автоматизированной верификации с применением инструментов Rodin и ProB // Прикладная дискретная математика. 2021. № 52. С. 83-96. / P. N. Devyanin, M. A. Leonova, “The techniques of formalization of OS Astra Linux Special Edition access control model using Event-B formal method for verification using Rodin and ProB”, Prikl. Diskr. Mat., 2021, no. 52, pp. 83–96 (In Russian).

[13]. Девянин П.Н., Хорошилов А.В., Тележников В.Ю. Формирование методологии разработки безопасного системного программного обеспечения на примере операционных систем. Труды ИСП РАН, том 33, вып. 5, 2021, стр. 25-40 / Devyanin P.N., Telezhnikov V.Y., Khoroshilov V.V. Building a methodology for secure system software development on the example of operating systems. Trudy ISP RAN/Proc. ISP RAS, vol. 33, issue 5, 2021, pp. 25-40 (in Russian).

[14]. Девянин П.Н. Результаты переработки уровней ролевого управления доступом и мандатного контроля целостности формальной модели управления доступом ОС Astra Linux. Труды ИСП РАН, том 35, вып. 5, 2023, стр. 7-22 / Devyanin P.N. The results of reworking the levels of role-based access control and mandatory integrity control of the formal model of access control in Astra Linux. Trudy ISP RAN/Proc. ISP RAS, vol. 35, issue 5, 2023, pp. 7-22 (in Russian).

## Информация об авторах / Information about authors

Петр Николаевич ДЕВЯНИН – член-корреспондент Академии криптографии России, доктор технических наук, профессор, научный руководитель ООО "РусБИТех-Астра" («Группа Астра»). Область интересов: теория информационной безопасности, формальные модели безопасности компьютерных систем, разработка безопасного программного обеспечения, операционные системы семейства Linux.

Petr Nikolaevich DEVYANIN – Doctor of Technical Sciences, corresponding member of Russian Academy of Cryptography, professor, scientific director in RusBITech-Astra (Astra Linux). Field of Interest: information security theory, formal security models of computer systems, secure software development, operating systems of Linux family.