О РЕЗУЛЬТАТАХ АПРОБАЦИИ ПРОЕКТА НАЦИОНАЛЬНОГО СТАНДАРТА ГОСТ Р «ЗАЩИТА ИНФОРМАЦИИ. ФОРМАЛЬНОЕ МОДЕЛИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ» НА ПРИМЕРЕ ОССН ASTRA LINUX SPECIAL EDITION

чл.-корр. АК России, д.т.н., профессор Девянин П.Н.
к.ф.-м.н. Хорошилов А.В.

ТРЕБОВАНИЯ ФСТЭК РОССИИ

- **ГОСТ Р ИСО/МЭК 15408-2013 «КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»** – формальная модель политики безопасности (ОУД6);
- **ГОСТ Р 56939-2016 «ЗАЩИТА ИНФОРМАЦИИ. РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ОБЩИЕ ТРЕБОВАНИЯ»** – статический и динамический анализ кода программ, фаззинг-тестирование программ;
- **ПРИКАЗ ОТ 19.08.2016 № 119 «ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ К ОПЕРАЦИОННЫМ СИСТЕМАМ» (ПРОФИЛИ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ)** – анализ скрытых каналов (5 класс защиты), формальная модель политики безопасности (3 класс защиты);
- **ПРИКАЗ ОТ 30.07.2018 № 131 «ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ, УСТАНАВЛИВАЮЩИЕ УРОВНИ ДОВЕРИЯ К СРЕДСТВАМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И СРЕДСТВАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»** – анализ скрытых каналов по памяти и по времени, формальная модель политики безопасности и ее верификация;
- **МЕТОДИКА ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ (УТВЕРЖДЕНА 11.02.2019)** – статический и динамический анализ кода, символьное выполнение, анализ трасс, SMT-решатели, фаззинг

ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ, УСТАНАВЛИВАЮЩИЕ 6 УРОВНЕЙ ДОВЕРИЯ (ПРИКАЗ ФСТЭК РОССИИ ОТ 30.07.2018 № 131)

5 УРОВЕНЬ ДОВЕРИЯ (ОБЪЕКТЫ КИИ 2 КАТЕГОРИИ, ГИС 2 КЛАССА ЗАЩИЩЕННОСТИ)

- идентификация и анализ скрытых каналов по памяти.

4 УРОВЕНЬ ДОВЕРИЯ (ОБЪЕКТЫ КИИ 1 КАТЕГОРИИ, ГИС 1 КЛАССА ЗАЩИЩЕННОСТИ)

- модель безопасности, включая реализуемые политики управления доступом и фильтрации информационных потоков.

3 УРОВЕНЬ ДОВЕРИЯ (ИС, В КОТОРЫХ ОБРАБАТЫВАЕТСЯ ИНФОРМАЦИЯ, СОДЕРЖАЩАЯ СЕКРЕТНЫЕ СВЕДЕНИЯ)

- верификация модели безопасности с использованием инструментальных средств;
- идентификация и анализ скрытых каналов по времени.

1 УРОВЕНЬ ДОВЕРИЯ (ИС, В КОТОРЫХ ОБРАБАТЫВАЕТСЯ ИНФОРМАЦИЯ, СОДЕРЖАЩАЯ СВЕДЕНИЯ ОСОБОЙ ВАЖНОСТИ)

- идентификация и анализ скрытых статистических каналов.

НИР ПО РАЗРАБОТКЕ ПРОЕКТОВ ГОСТ Р «ЗАЩИТА ИНФОРМАЦИИ. ФОРМАЛЬНОЕ МОДЕЛИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ»

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р
(проект, окончательная редакция)

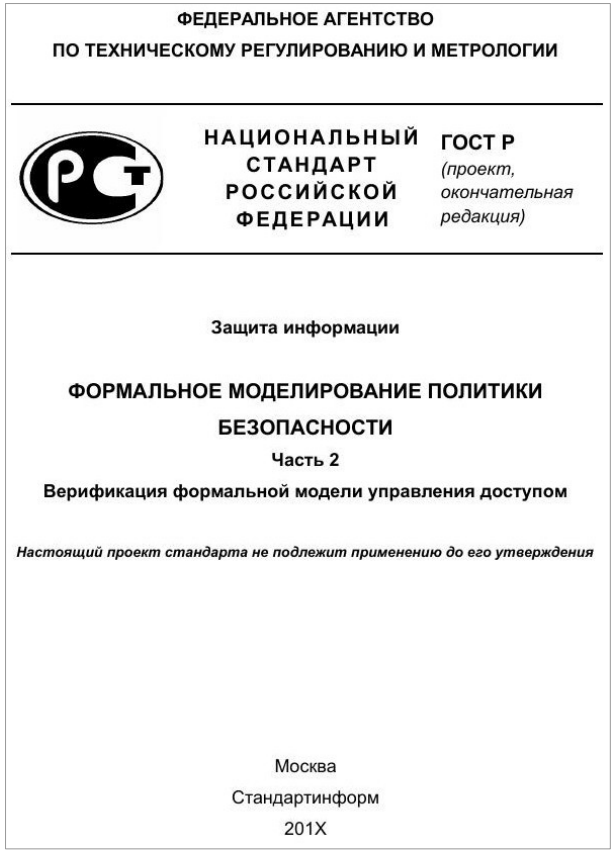
Защита информации

ФОРМАЛЬНОЕ МОДЕЛИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ
Часть 1
Формальная модель управления доступом

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
201X

СОДЕРЖАНИЕ



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р
(проект, окончательная редакция)

Защита информации

ФОРМАЛЬНОЕ МОДЕЛИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ
Часть 2
Верификация формальной модели управления доступом

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
201X

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЕ МАНДАТНОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ (МКЦ)

ПОЛИТИКА МАНДАТНОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ; ПОЛИТИКА МАНДАТНОГО КОНТРОЛЯ ДОВЕРИЯ: Политика управления доступом, при реализации которой задаются уровни целостности (классификационные метки): каждому объекту доступа присваивается уровень целостности, отражающий доверие к целостности содержащейся в нем информации, каждому субъекту присваивается уровень целостности, отражающий его полномочия по доступу к объектам доступа в зависимости от их уровней целостности и доверие к его функциональности; субъект может получить доступ к объекту доступа или другому субъекту только в случае, когда выполняются следующие правила:

- при получении доступа на запись к объекту доступа уровень целостности субъекта должен быть не ниже уровня целостности объекта доступа;
- доступ субъекта к объекту доступа или другому субъекту не приводит к получению субъектом контроля над некоторым субъектом, уровень целостности которого не сравним или выше уровня целостности первого субъекта.

МОДЕЛИРОВАНИЕ СОСТОЯНИЙ АБСТРАКТНОГО АВТОМАТА НА ПРИМЕРЕ МКЦ

ФОРМАЛЬНОЕ ОПИСАНИЕ СОСТОЯНИЙ АБСТРАКТНОГО АВТОМАТА 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, сущностей;
- множества учетных записей привилегированных и непривилегированных пользователей;
- множества привилегированных и непривилегированных субъектов;
- множества, функции (отношения), используемые для задания сущностей, функционально ассоциированных с субъектами;
- множества, функции (отношения), используемые для задания субъектов, контролируемых другими субъектами;
- множества, функции (отношения), используемые для задания контейнеров, доступ к содержащимся в которых сущностям субъектам может быть разрешен без учета уровней целостности таких контейнеров.

Пример

$(LI, \leq)$ – решетка уровней целостности, где $\leq$ – 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, $N_S \subseteq S$ – множество непривилегированных субъектов, 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 каждой сущности;
$i_s: S \to LI$ – функция, задающая уровень целостности каждого субъекта;
$[s] \subset E$ – множество сущностей, функционально ассоциированных с субъектом $s \in S$;
$control: S \to 2^S$ – функция, задающая для каждого субъекта множество контролируемых (управляемых) им субъектов;
$CCRI: C \to \{true, false\}$ – функция, задающая способ доступа к сущностям внутри контейнеров с учетом их уровней целостности, где если доступ к сущностям, содержащимся внутри контейнера $c \in C$, разрешен без учета его уровня целостности, то по определению выполняется равенство $CCRI(c) = false$, в противном случае выполняется равенство $CCRI(c) = true$.

МОДЕЛИРОВАНИЕ СОСТОЯНИЙ АБСТРАКТНОГО АВТОМАТА НА ПРИМЕРЕ 2 УРОВНЯ (МКЦ) МРОСЛ ДП-МОДЕЛИ ДЛЯ ОССН

$R_f = \{write_m\}$ – множество видов информационных потоков;
$F \subseteq (E \cup S) \times (E \cup S) \times R_f$ – множество информационных потоков;
$(LI, \leq)$ – решётка уровней целостности данных;
$(i_u, i_e, i_r, i_s) \in I$ – четвёрка функций уровней целостности, при этом:
$i_u: U \to LI$ – функция, задающая для каждой учётной записи пользователя её уровень целостности;
$i_e: E \to LI$ – функция, задающая уровень целостности для каждой сущности;
$i_r: R \cup NR \cup AR \to LI$ – функция, задающая для каждой роли её уровень целостности;
$i_s: S \to LI$ – функция, задающая для каждой субъект-сессии её текущий уровень целостности;
I – множество всех четверок функций заданного вида;
$CCRI: E \cup R \cup NR \cup AR \to \{true, false\}$ – функция, задающая способ доступа к сущностям внутри контейнеров;
$check\_i\_right: S \times (E \cup R \cup NR \cup AR \cup S) \times R_r \to 2^{R \cup NR \cup AR}$ – функция наличия права доступа у текущих ролей субъект-сессии к сущности, роли или субъект-сессии с учетом мандатного контроля целостности;
$execute\_i\_container: S \times E \to \{true, false\}$ – функция доступа субъект-сессии к сущностям в контейнерах;
$G = (APA, PA, user, (i_u, i_e, i_r, i_s), CCRI, A, AA, F, H_R, H_E, H_S, constraint_{NR})$ – состояние системы;
$]u[\subset E$ – множество сущностей, параметрически ассоциированных с учётной записью пользователя $u \in U$;
$]s[\subset E$ – множество сущностей, параметрически ассоциированных с субъект-сессией $s \in S$;
$fp: U \times E \to 2^E$ – функция, задающая множества сущностей, параметрически ассоциированных с субъект-сессией при её создании из сущности от имени учётной записи пользователя;
$[s] \subset E$ – множество сущностей, функционально ассоциированных с субъект-сессией s;
$fa: U \times E \to 2^E$ – функция, задающая множества сущностей, функционально ассоциированных с субъект-сессией при её создании от имени учётной записи пользователя из сущности;
$]r[\subset E$ – множество сущностей, параметрически ассоциированных с ролью;
$de\_facto\_own: S \to 2^S$ – функция де-факто владения субъект-сессиями

МОДЕЛИРОВАНИЕ ПЕРЕХОДОВ АБСТРАКТНОГО АВТОМАТА ИЗ СОСТОЯНИЙ В СОСТОЯНИЯ НА ПРИМЕРЕ МКЦ

ДОЛЖНЫ БЫТЬ ФОРМАЛЬНО ОПИСАНЫ ПРАВИЛА ПЕРЕХОДА АБСТРАКТНОГО АВТОМАТА ИЗ СОСТОЯНИЙ В СОСТОЯНИЯ:

- для задания и (или) изменения уровней целостности учетных записей пользователей или субъектов;
- для задания и (или) изменения уровней целостности сущностей;
- для получения субъектами контроля над другими субъектами за счет использования информационных потоков по памяти к сущностям, функционально ассоциированным с субъектами.

Пример. Правило захвата контроля субъектом над другим субъектом

Параметры правила:

x, y – субъекты;

z – сущность.

Условия применения правила:

$x, y \in S$ – субъекты 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;

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

Результаты применения правила:

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

МОДЕЛИРОВАНИЕ ПЕРЕХОДОВ АБСТРАКТНОГО АВТОМАТА ИЗ СОСТОЯНИЙ В СОСТОЯНИЯ НА ПРИМЕРЕ 2 УРОВНЯ (МКЦ) МРОСЛ ДП-МОДЕЛИ ДЛЯ ОССН

access_write(x, x', y)		
x, y	$x \in S, y \in E \cup R \cup NR \cup AR$	если $y \in E$, то $A' = A \cup \{(x, y, write_a)\}$, если $y \in R \cup NR \cup AR$, то $AA' = AA \cup \{(x, y, write_a)\}$
x'	$x' \in S, \varnothing \neq check\_i\_right(x, y, write_r) \subset R \cup AR$, [если $y \in E$, то $execute\_i\_container(x, y) = true$], [если $y \in R \cup NR \cup AR$, то для $e \in]y[$ либо $(x, e, read_a) \in A$, либо $(x, e, write_a) \in A$], [если ($y \in E \setminus \{i\_entity\}$ и $i_e(y) > i\_low$) или ($y \in R \cup NR \cup AR$ и $i_r(y) > i\_low$), то $(x', i\_entity, write_a) \in A$]	–
take_access_own(x, y, z)		
–	–	–
x, y, z	$x \in N_S, y, z \in S, y \in de\_facto\_own(x)$, [$z \in de\_facto\_own(y)$ или $((y, z, write_m) \in F$, $\varnothing \neq check\_i\_right(y, z, own_r) \subset R \cup AR)$]	$de\_facto\_own'(x) = de\_facto\_own(x) \cup \{z\}$

ДОКАЗАТЕЛЬСТВО ВЫПОЛНЕНИЯ В АБСТРАКТНОМ АВТОМАТЕ УСЛОВИЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ МКЦ

УСЛОВИЯ БЕЗОПАСНОСТИ АБСТРАКТНОГО АВТОМАТА, РЕАЛИЗУЮЩЕГО МКЦ:

- определяющие допустимые уровни целостности субъектов в зависимости от уровней целостности учетных записей пользователей, от имени которых они функционируют;
- определяющие допустимые уровни целостности сущностей в составе контейнеров;
- определяющие допустимые уровни целостности для сущностей, функционально ассоциированных с субъектами, в зависимости от уровней целостности субъектов;
- возможности контроля одного субъекта над другим субъектом в зависимости от их уровней целостности;
- безопасности информационных потоков.

МАТЕМАТИЧЕСКОЕ (ФОРМАЛЬНОЕ) ДОКАЗАТЕЛЬСТВО того, что при выполнении условий безопасности абстрактного автомата, реализующего мандатный контроль целостности, в абстрактном автомате невозможно получение непривилегированным субъектом контроля над другим субъектом в случае, когда уровень целостности первого субъекта не сравним или меньше уровня целостности второго субъекта.

Примеры

Допустимые уровни целостности сущностей в составе контейнеров:

- *для сущностей $x, y \in E$, если $x \in H_E(y)$, то $i_e(x) \leq i_e(y)$ – уровень целостности сущности не выше уровня целостности контейнера, в котором она содержится.*

Условия безопасности информационных потоков:

- *для сущностей $x, y \in E$, если $x \in H_E(y)$, то $i_e(x) \leq i_e(y)$ – уровень целостности сущности не выше уровня целостности контейнера, в котором она содержится;*
- *для каждого информационного потока $(x, y, write_m) \in F$ справедливо неравенство $i_e(y) \leq i_e(x)$ – разрешены только информационные потоки по памяти, когда сущность-приемник имеет уровень целостности не выше уровня целостности сущности-источника.*

ДОКАЗАТЕЛЬСТВО ВЫПОЛНЕНИЯ В АБСТРАКТНОМ АВТОМАТЕ УСЛОВИЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ 2 УРОВНЯ (МКЦ) МРОСЛ ДП-МОДЕЛИ ДЛЯ ОССН

ОПРЕДЕЛЕНИЕ. Пусть G_0 – безопасное начальное состояние системы $\Sigma(G^*, OP, G_0)$, и существует траектория без кооперации доверенных и недоверенных субъект-сессий $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N$, где $N \geq 1$. Будем говорить, что в состоянии G_N произошло нарушение безопасности системы в смысле мандатного контроля целостности, когда существуют недоверенная субъект-сессия $x \in N_{SN}$ и субъект-сессия $y \in de\_facto\_own_N(x)$ такие, что не верно неравенство $i_s(y) \leq i_s(x)$, и это условие не выполняется в состояниях G_i траектории, где $0 \leq i < N$. Назовём систему $\Sigma(G^*, OP, G_0)$ безопасной в смысле мандатного контроля целостности, когда в ней невозможно соответствующее нарушение безопасности.

ТЕОРЕМА. Пусть G_0 – безопасное начальное состояние системы $\Sigma(G^*, OP, G_0)$. Пусть на всех траекториях системы без кооперации доверенных или недоверенных субъект-сессий $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N$, где $N \geq 0$, и в каждом состоянии G_N для каждой субъект-сессии $s \in S_N$ и сущности $e \in E_N$ выполняются следующие условия.

Условие Ц.1. Если $e \in [s]$, то выполняется условие $i_{sN}(s) \leq i_{eN}(e)$.

Условие Ц.2. Если $e \in]s[$, то $i_{sN}(s) \leq i_{eN}(e)$ и для каждой роли или административной роли $r \in R_N \cup AR_N$ такой, что $(e, read_r) \in PA_N(r)$, выполняется условие $i_{eN}(e) \leq i_{rN}(r)$.

Условие Ц.3. Для всех субъект-сессий $s \in S_N$ таких, что $i\_low < i_{sN}(s)$, выполняются условия $\{s' \in S_N \mid i\_low < i_{sN}(s') \leq i_{sN}(s)\} \times (E_N \cup S_N) \subset f\_correct_N(s)$, $\{s' \in S_N \mid i\_low < i_{sN}(s') \leq i_{sN}(s)\} \times (E_N \cup S_N) \subset p\_correct_N(s)$.

Тогда на этих траекториях система $\Sigma(G^*, OP, G_0)$ безопасна в смысле мандатного контроля целостности

ВЫБОР ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ВЕРИФИКАЦИИ ФОРМАЛЬНОЙ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ

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

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

ВЕРИФИКАЦИЯ ФОРМАЛИЗОВАННОГО (МАШИНОЧИТАЕМОГО) ОПИСАНИЯ ФОРМАЛЬНОЙ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ

ВЕРИФИКАЦИЯ С ПРИМЕНЕНИЕМ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДОЛЖНА СОСТОЯТЬ В ВЫПОЛНЕНИИ СЛЕДУЮЩИХ ДЕЙСТВИЙ:

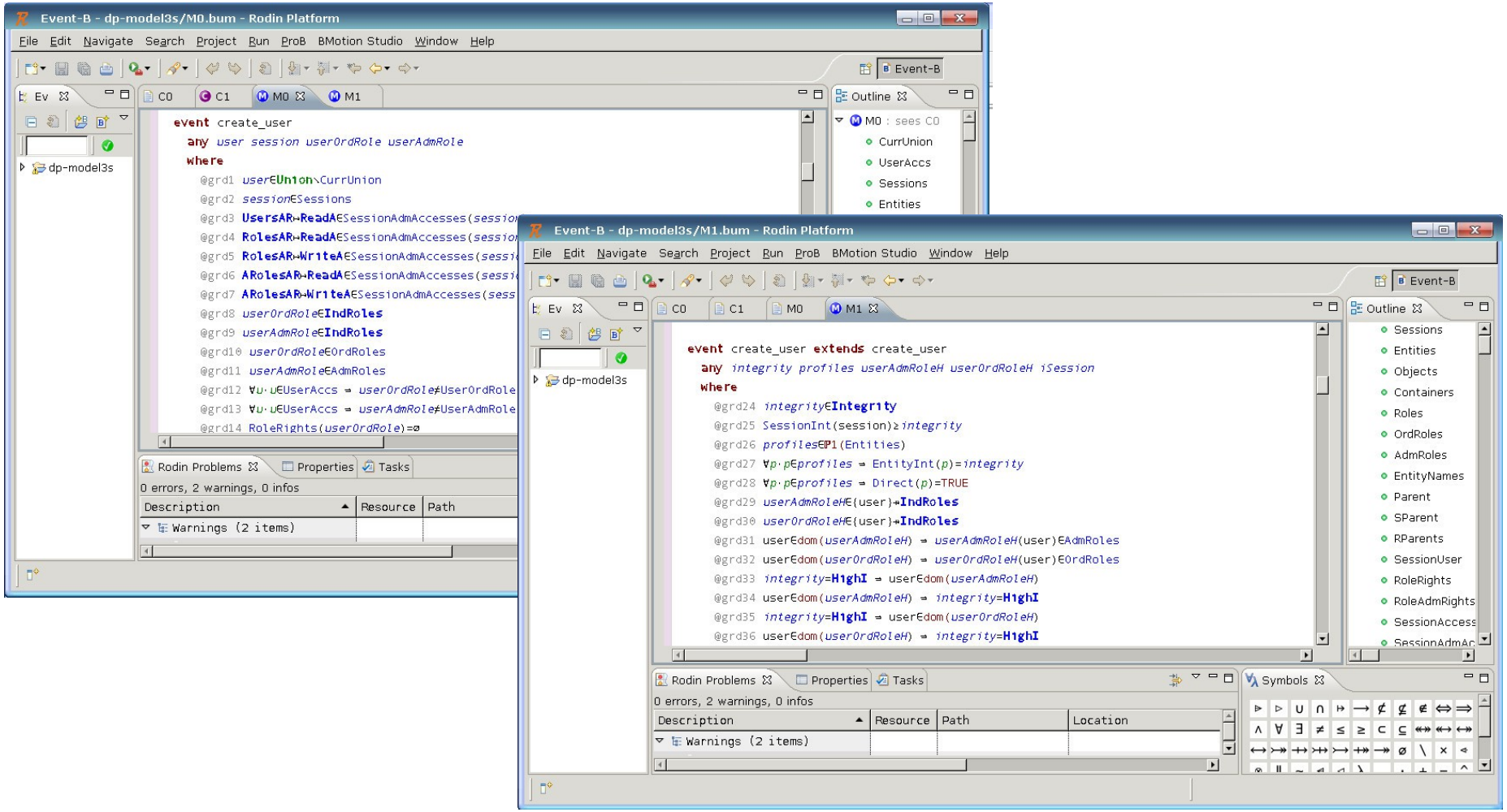
1. Должно быть осуществлено автоматическое доказательство непротиворечивости формальной модели и выполнения заданных в ее рамках условий безопасности (условий верификации) при наличии у инструментальных средств соответствующей функциональности, в противном случае должно быть выполнено интерактивное доказательство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

Примечание

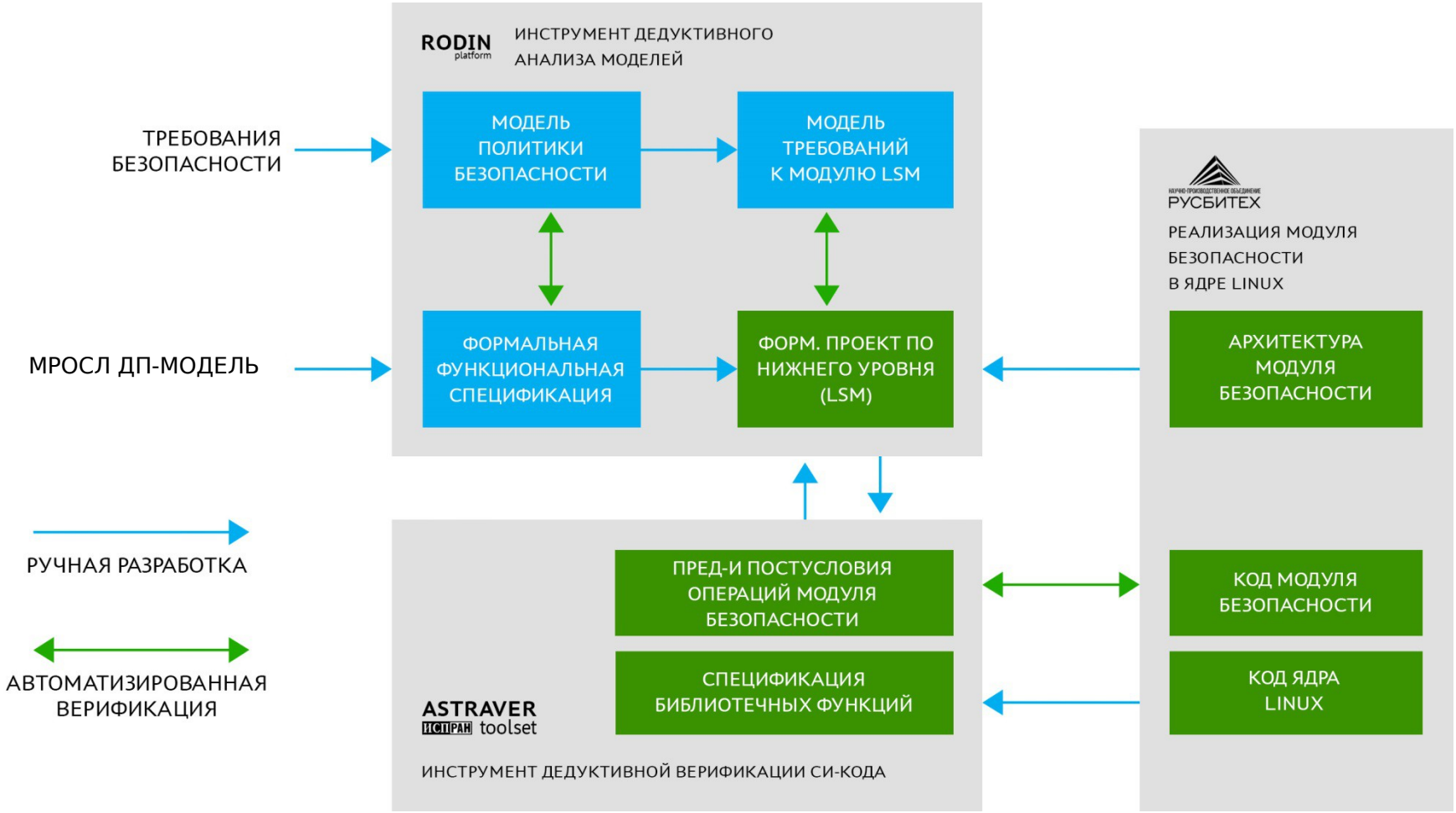
Возможными причинами невыполнения доказательства *условий верификации формальной модели управления доступом и путями их устранения являются:*

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

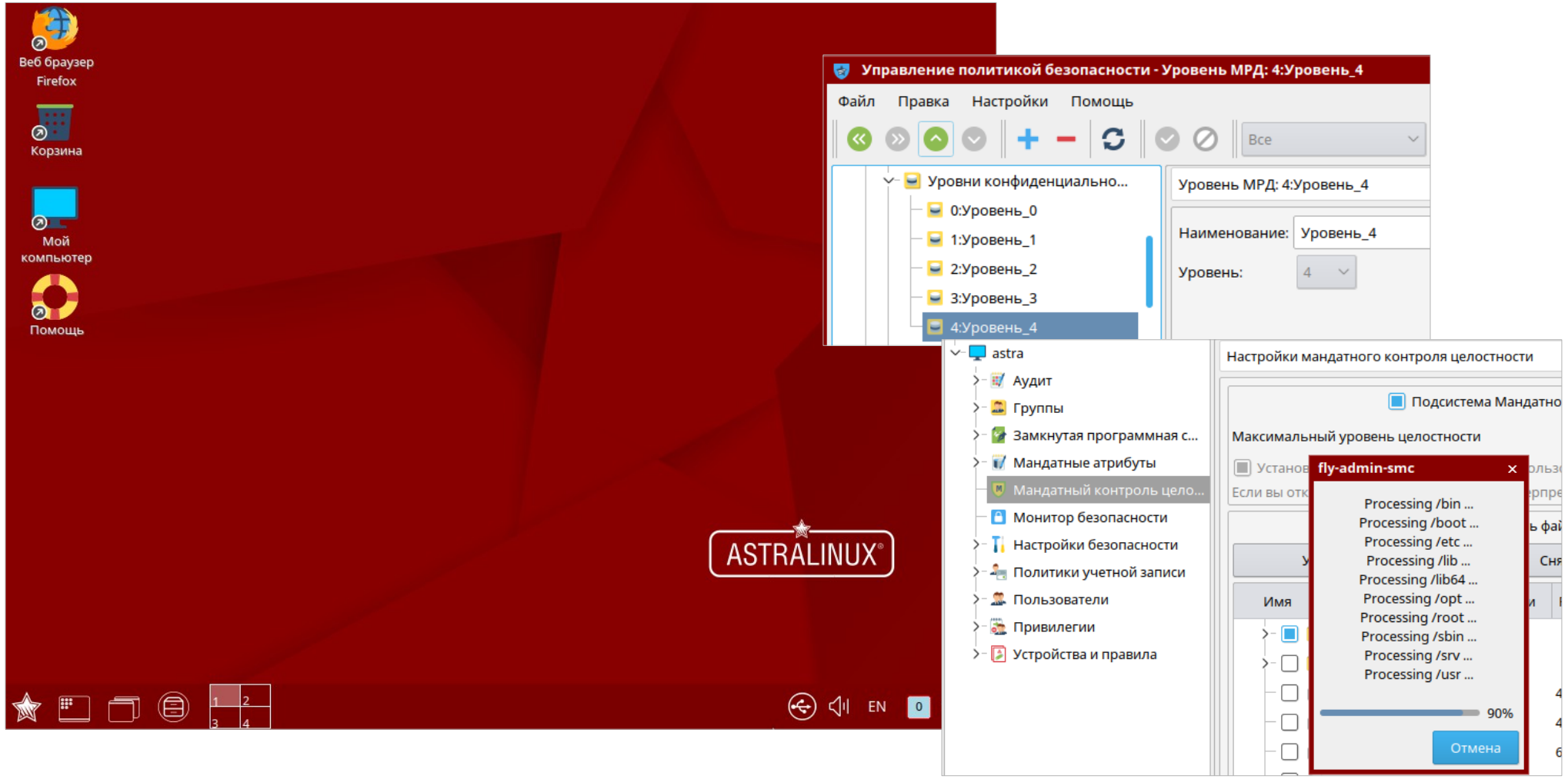
ПРИМЕР ВЕРИФИКАЦИИ ИНСТРУМЕНТАЛЬНЫМ СРЕДСТВОМ RODIN НА ФОРМАЛИЗОВАННОМ ЯЗЫКЕ EVENT-B 2 УРОВНЯ (МКЦ) МРОСЛ ДП-МОДЕЛИ



ВЕРИФИКАЦИЯ МРОСЛ ДП-МОДЕЛИ И ЕЁ РЕАЛИЗАЦИИ В ОССН С ПРИМЕНЕНИЕМ ИНТРУМЕТАЛЬНОГО СРЕДСТВА ASTRAVER TOOLSET



РЕАЛИЗАЦИЯ ВЕРИФИЦИРОВАННОЙ МРОСЛ ДП-МОДЕЛИ В ОССН ASTRA LINUX SPECIAL EDITION



ASTRA LINUX®

ИСП РАН

Спасибо за внимание!