doi: 10.36724/2409-5419-2021-13-6-50-59

ВЕРИФИКАЦИЯ СИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ МОДЕЛИРОВАНИЯ РАСКРАШЕННЫМИ СЕТЯМИ ПЕТРИ

ТИХОНОВ
Валерий Александрович[1]

НОВИКОВ
Владимир Александрович[2]

АННОТАЦИЯ

Введение: сложность разрабатываемых информационных систем повышает требования к безошибочному проектированию системы разграничения доступа и увеличивает вероятность наличия и влияние уязвимостей на состояние защищенности накапливаемой и обрабатываемой информации. Формальная верификация проекта информационной системы на этапе разработки позволяет минимизировать появление архитектурных уязвимостей. Изменения, проводимые регуляторами в области сертификации средств защиты информации, актуализируют вопросы, связанные с разработкой и анализом формальных моделей. **Цель исследования:** разработка подхода к построению и формальной верификации моделей, обладающего наглядностью, полнотой и результативностью анализа. **Методы:** построение моделей математическим аппаратом раскрашенных сетей Петри в среде моделирования CPN Tools с последующим исследованием свойств сети. **Результаты:** разработан подход, обладающий структурной, логической и динамической полнотой и непротиворечивостью. Наглядность моделей, разработанных с использованием представленного подхода, снижает время обнаружения некорректного функционирования и последующей разработки компенсирующих мер с последующим подтверждением их эффективности. Исследование пространства состояний показала необходимость дополнения среды моделирования решающими правилами для полного построения или расчета пространства состояний в случае сложных моделей и большого числа маркеров при начальной маркировке сети Петри. **Практическая значимость:** разработанный подход предлагается применять при формальной верификации моделей управления доступом и фильтрации потоков информации в процедуре сертификации средств защиты информации и при проектировании сложных информационных систем. Доказательность и простота подхода позволяет внедрить процедуру формальной верификации в этапы разработки различного рода систем. **Перспективы развития:** разработка дополнительного программного обеспечения, позволяющего строить полное пространство состояний для сложных моделей, а также дополнение метода подходами, использующими ASK-CTL логику.

Сведения об авторах:

[1]инженер-исследователь Акционерного общества "Технологии радиоконтроля" г. Санкт-Петербург, Россия, v.tihonov@ao-trk.ru

[2]д.т.н. Лауреат премии Президента РФ в области науки и инноваций Начальник испытательного центра Акционерного общества "Технологии радиоконтроля", г. Санкт-Петербург, Россия, v.novikov@ao-trk.ru

КЛЮЧЕВЫЕ СЛОВА: *формальная верификация, информационная безопасность, раскрашенные сети Петри, моделирование, оценка соответствия.*

Для цитирования: Тихонов В.А., Новиков В.А., Верификация систем управления доступом на основе моделирования раскрашенными сетями Петри // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 6. С. 50-59. doi: 10.36724/2409-5419-2021-13-6-50-59

Введение

В реализации современных проектов неотъемлемую часть занимают информационные технологии. Программное обеспечение используется для автоматизации и управления деятельностью, обработки и передачи информации как в коммерческих компаниях, так и в государственных структурах. Практически непрерывный рост объема данных, критичность информации и объемы задач, решаемые при автоматизации различных процессов, приводят к недостаточной проработке вопроса управления разграничением доступа и, как следствие, появлению архитектурных неустранимых уязвимостей.[1],[2] В последние годы, для уменьшения количества уязвимостей в программном обеспечении средств защиты информации [3] в процедуру сертификации внесен этап формальной верификации. Он требует наличия и исследования формальной модели для механизмов, реализующих управление доступом и фильтрацию информационных потоков. Авторами проанализированы различные подходы и изучены среды, позволяющие выполнять верификацию механизмов разграничения доступом. Применяющиеся методы формальной верификации моделей управления доступом, характеризуются высоким порогом вхождения, не обладают наглядностью и сложны с точки зрения внесения изменений для коррекции или адаптации. В связи с этим был развит подход, основанный на аппарате раскрашенных сетей Петри снижающий влияние известных недостатков.

Описание подхода

Разработанный подход основан на соответствии модели структурным, логическим и динамическим характеристикам исследуемой системы.[4] В данном случае и далее, под системой понимается разрабатываемая информационная система, программное обеспечение или их составные части. Математическим аппаратом, используемым для построения моделей, является аппарат раскрашенных сетей Петри.[5][6] Раскрашенные сети Петри — это расширение классических сетей петри описанных в [7].

Структура модели определяется составом элементов и их взаимосвязью. Она должна соответствовать описанию, приведенному в конструкторской документации (в ряде случаев в задании по безопасности), на основе которой разрабатывается система. Для соблюдения этого требования элементы модели сопоставляются с элементами, составляющими функциональные требования системы. Таким образом, полное соответствие элементов модели и элементов функциональных требований позволяет доказать структурное соответствие модели и системы. Структурной характеристикой в аппарате сетей Петри является ориентированный двудольный граф.

Логическая составляющая модели задаётся после формирования структуры модели в виде набора взаимосвязанных условий функционирования сети Петри – правил срабатывания переходов. Данные условия формулируются до начала моделирования и соответствуют условиям, определяющим работу механизмов и свойства исследуемой системы.

Динамической характеристикой модели являются её поведенческие особенности в процессе имитационного моделирования. Корректно построенная модель в процессе моделирования находится в состояниях, соответствующих состояниям исследуемой системы. При этом осуществляется подтверждение корректности системы за счет доказательства нахождения системы в безопасных состояниях. Безопасные состояния формируются на основе условий и свойств функционирования, описанных в конструкторской документации. Так, например, для классической модели мандатного управления доступом безопасные состояния — это состояния, в которых выполняются правила простой безопасности, *-правило и правило дискреционной безопасности.[8]

Сформированная с учётом описанных характеристик модель исследуется с помощью различного рода симуляций и анализа пространства состояний. На основе пространства состояний определяется наличие или отсутствие запрещенных траекторий функционирования системы. Симуляция позволяет наглядно продемонстрировать запрещенные варианты функционирования системы, а также при внесении дополнительных элементов, моделирующих различного рода нарушения изучить влияние этих нарушений на систему в целом, оценить последствия рисков проявления нарушений и действенность угроз.

Построение модели

Для подтверждения практической значимости и корректности разработанного метода приведен пример создания и анализа модели системы, основанной на классической модели с мандатным управлением доступа Белла-ЛаПадулы. Выбор классической модели обоснован её широкой известностью в научных кругах. [9][10] Для построения и анализа раскрашенных сетей Петри используется инструмент CPN Tools. CPN Tools предназначен для разработки, симуляции и анализа раскрашенных сетей Петри. [11][12] Выбор средства обоснован широким функционалом и возможностью добавлять собственные плагины, расширяющие сферу применения. [13][14][15].

На основании формального описания модели Белла-ЛаПадулы сформированы множества цветов (colorset – в рамках CPN Tools), соответствующие множествам классической модели. При этом на основе атомарных цветов, определяющих базовые элементы модели, сформированы составные цвета, моделирующие более сложные сущности, необходимые для построения модели. Далее определены необходимые структурные элементы сети Петри – позиции и переходы. Позиции являются элементами накопления и отображения, а переходы элементами, моделирующими события в системе. Набор позиций и переходов определяется по формальному описанию элементов системы и содержит минимально необходимые элементы, значимые для системы. При этом возможность использования подходов иерархичной разработки облегчает задачу построение сети Петри. [16][17][18][19] Построенный граф сети Петри с учётом описанного выше представлен на рисунках 1-5.

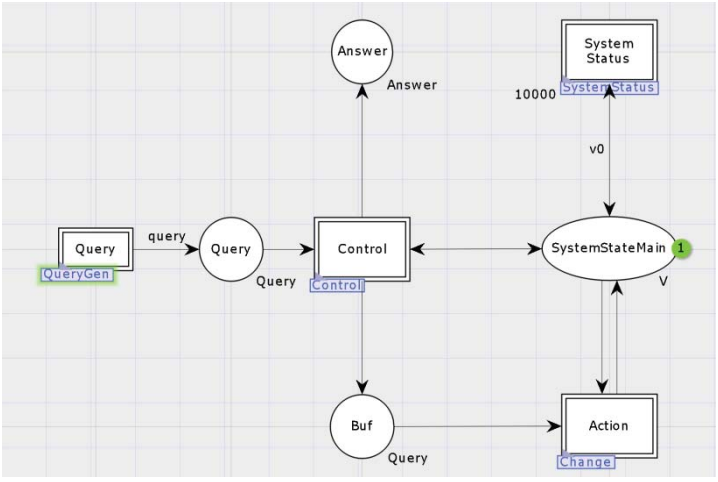


Рис. 1. Верхний уровень сети Петри модели Белла-ЛаПадулы

Данная сеть Петри является верхним уровнем модели и отображает основные части системы, реализующие её функционирование: запрос, проверка запроса на корректность, изменение состояния системы. Переходы-замещения, соответственно “Query”, “Control”, “Action”.

Позиция “SystemStateMain” моделирует текущее состояние системы. Маркер данной позиции является составным и отображает текущее состояние системы описываемое:

– существующими доступами в системе;
– матрицей доступа;
– текущим множеством функций конфиденциальности.

Позиция “Answer” предназначена для отображения отрицательного ответа системы на возникающий запрос добавления доступа в состояние системы. Позиции “Query” и “Buf” являются позициями, объединяющими разные подсети Петри и предназначены для передачи запросов между элементами модели.

Переход “Query” моделирует возникновение запроса. При этом он является переходом-замещением и содержит «вложенную» сеть Петри, представленную на рисунке 2.

Позиции и переходы, представленные на рисунке 2, моделируют запросы к системе на:

– изменение множества текущих доступов,
– изменение функции конфиденциальности,
– изменение прав доступа в матрице.

Маркеры, содержащиеся в данных позициях, моделируют соответствующие типу позиции запросы в системе. Позиции “St” являются вспомогательными и предназначены для отображения типа запроса и устранения коллизий запросов.

Переход “Control” на рисунке 1 моделирует контроль запроса на изменение множества текущих доступов в соответствии с правилами классической мандатной модели. При этом он является переходом-замещением и содержит «вложенную» сеть Петри, представленную на рисунке 3.

Позиция “In2” является входной позицией подсети и содержит проверяемый запрос. Позиция “V” является позицией, моделирующей текущее состояние системы и, по своей сути, является позицией “ SystemStateMain ” из сети Петри, изображенной на рисунке 1.

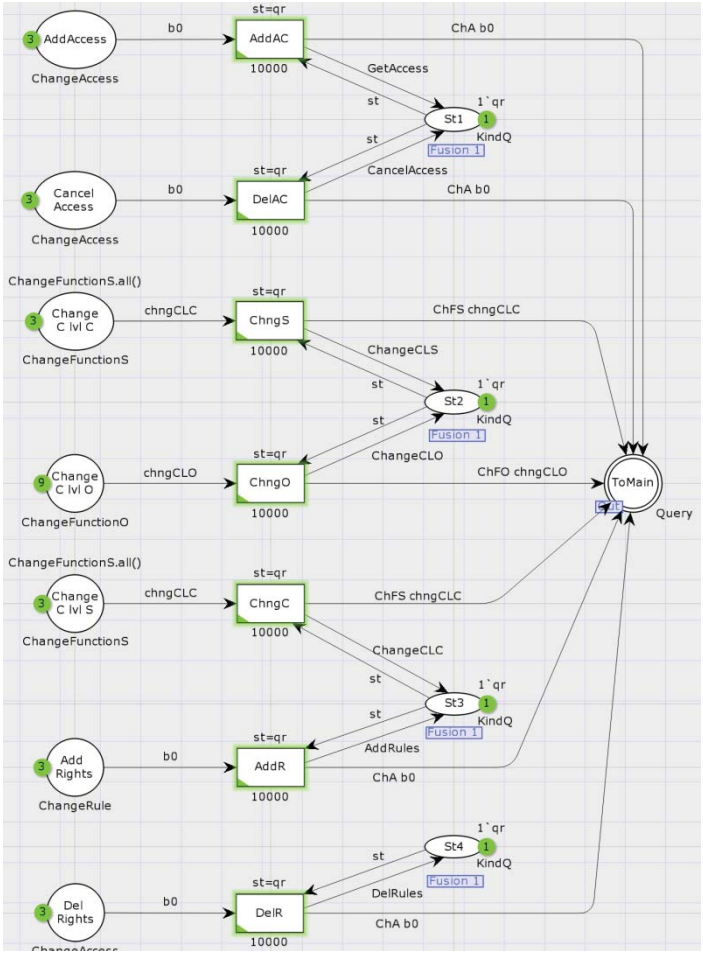


Рис. 2. Сеть Петри, моделирующая поступление запроса

Позиция “Out” является позицией, содержащей результат проверки соответствия запроса правилам безопасности. Позиция “Buf” является позицией, предназначенной для передачи запроса на следующий элемент сети Петри верхнего уровня, реализующей изменения состояния системы. По сути является позицией “Buf” из сети Петри, изображенной на рисунке 1, а позиция “Out” позицией “Answer”.

Переходы “SS Property”, “ Star Property” и “DS-Property” моделируют нарушение правил «Простой безопасности», «*-правила» и «Дискреционного правила» соответственно. При возникновении нарушения маркер моделирующий запрос помещается в позицию “Out” и дальнейшая обработка запроса прекращается. Таким образом, изменение в множество текущих доступов не вноситься. Переход “ALL OK” моделирует корректность запроса относительно перечисленных ранее правил и помещает маркер, моделирующий запрос в позицию “Buf”.

Переход “Action” на рисунке 1 моделирует изменение состояния системы в соответствии с правилами классической мандатной модели. При этом он является переходом-замещением и содержит «вложенную» сеть Петри, представленную на рисунке 4.

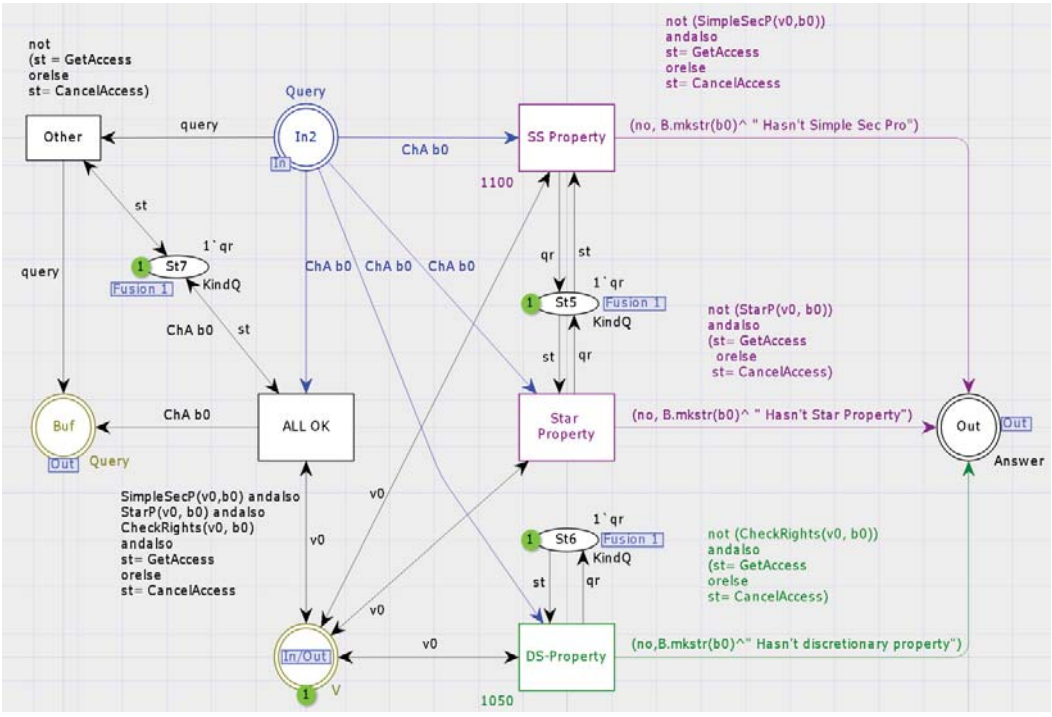


Рис. 3. Сеть Петри, моделирующая проверку соответствия правилам

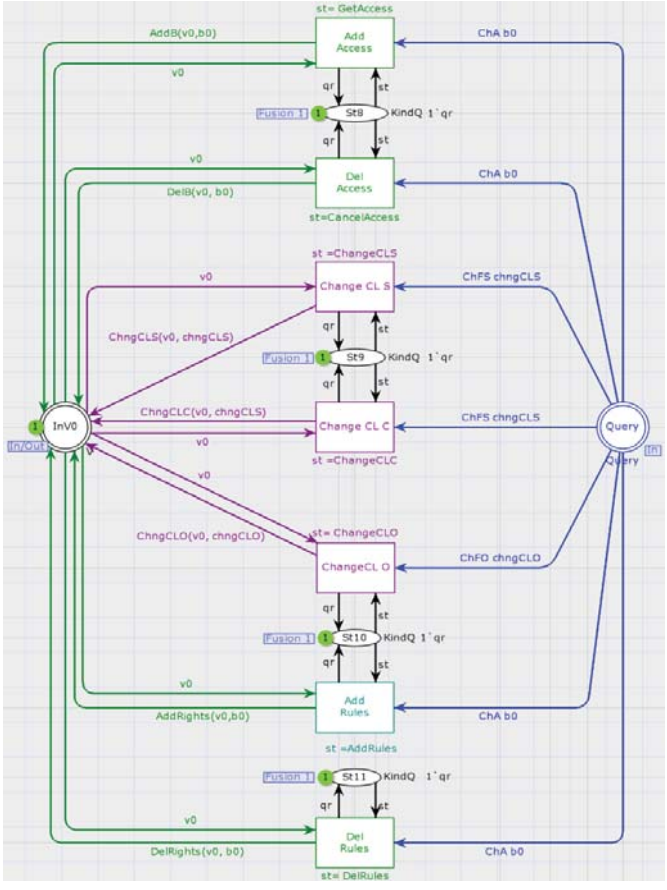


Рис. 4. Сеть Петри, моделирующая изменения в текущем состоянии системы

Позиция “InV0” является позицией, моделирующей текущее состояние системы, по своей сути является позицией “SystemStateMain” из сети Петри, изображенной на рисунке 1. Позиция “Query” моделирует поступление запроса и по своей сути является позицией “Buf” из сети Петри, изображенной на рисунке 1.

Сеть Петри, изображенная на рисунке 5 предназначена для контроля безопасного состояния системы.

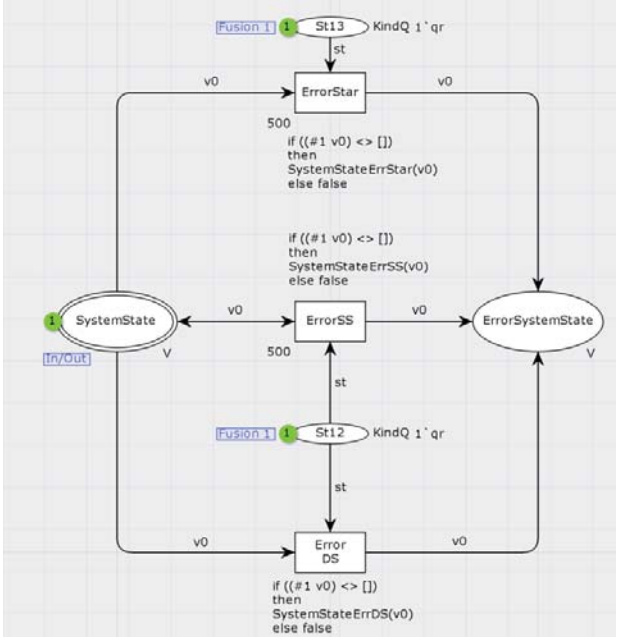


Рис. 5. Сеть Петри, моделирующая контроль текущего состояния системы

Позиция “System State” на рисунке 5 моделирует текущее состояние системы по своей сути является позицией “SystemStateMain” из сети Петри, изображенной на рисунке 1. Позиция “ErrorSystemState” отображает нарушение безопасного состояния системы при текущих доступах и в случае корректного функционирования системы остаётся всегда пустой.

Переходы “ErrorStar”, “ErrorSS”, “Error DS” моделируют нарушение свойств безопасности в текущих доступах.

Анализ модели

При исследовании модели применяется анализ пространства состояний. [20], [21] Поскольку известной проблемой в сетях Петри является комбинаторный взрыв при большой начальной маркировке внесены ограничения для модели. Начальная маркировка, а следовательно входные данные, формировались с учетом следующих ограничений:

– Исследовались свойства сохранности правил «Простой безопасности» и «*-правила» при изменении состояния системы.

– Множество субъектов ограничено одним элементом.

– Для множества доступов проводились исследования на одном, двух и трёх видах доступа.

При анализе пространства состояний использовались штатные средства моделирования.

Для одного вида доступа получено полное пространство состояния модели, насчитывающее 71619 узлов, из них конечными являлись 41423 узла. На основе автоматизированного анализа конечных узлов пространства состояний обнаружено 2372 конечных узла с нарушениями. Наличие нарушения определялось на основе итоговой маркировки позиции “ErrorSystemState”. В корректно работающей системе данная позиция остаётся с пустой маркировкой, что говорит о сохранности безопасного состояния системы и корректности работы сформулированных в классической модели правил.

На рисунке 6 изображена одна из траекторий, приводящая к состоянию системы, нарушающему условия безопасности. Снизу под траекторией представлено описание некоторых дуг пространства состояний (.При) при этом полем 1 обозначена информация о связи узлов, в поле 2 – переход, создавший изменения в состоянии, а полем 3 изменения, вносимые в маркировку сети.

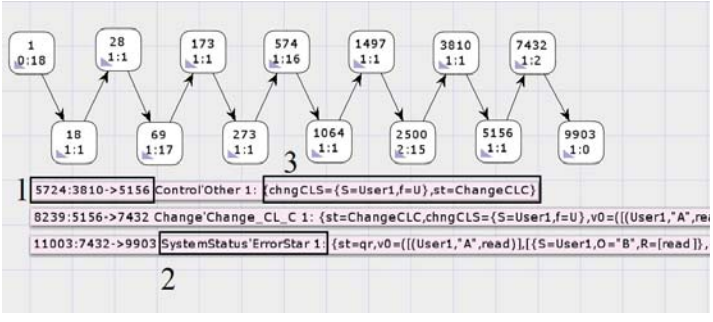


Рис. 6. Траектория нарушения условий безопасности

Каждый узел содержит информацию о текущем состоянии системы и средствами среды моделирования возможно воспроизвести любое из имевших место состояний в симулятор для дальнейшего исследования событий, вызвавших нарушения. Например, при анализе в симуляторе узла 7432, предпоследнего узла на рисунке 6, активными являются переходы “ErrorStar” и “ErrorSS”, что говорит о наличии запрещенных доступов и, следовательно, потоков информации.

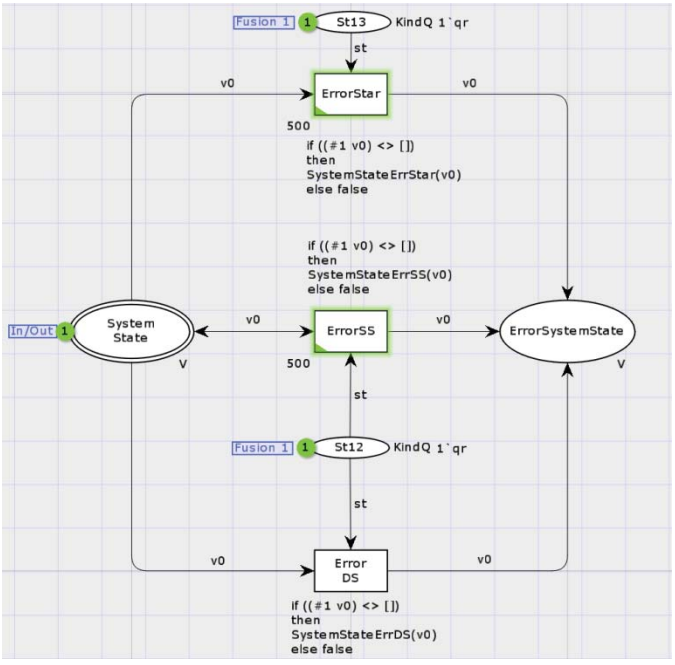
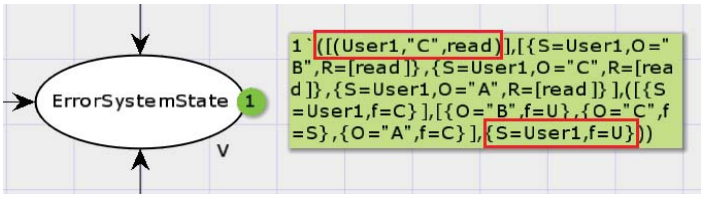


Рис. 7. Маркировка подсети для 7432 узла пространства состояний

Для подробного изучения модели в процессе симуляций просматриваются текущие значения маркеров в позициях. На рисунке 8 изображена позиция “ErrorSustemState” с отображением конечной маркировки, моделирующей состояние системы с нарушением, и позиции “SystemStateMain” с начальной маркировкой.



а) Конечное состояние системы, нарушающее условия безопасности

б) Конечное состояние системы

Рис. 8. Визуализация содержания маркеров

Виды симуляции, реализованные в среде моделирования, позволяют проводить пошаговую симуляцию без выбора маркеров, проходящих через переход сети Петри, и с выбором маркера для более подробного изучения влияния частных маркировок. Также реализована автоматическая симуляция заданного числа шагов с отображением каждого шага моделирования и без отображения с выводом итоговой маркировки. Описанные инструменты позволяют наглядно оценить траектории, приводящие к нарушениям исследуемых свойств. Сформировать недопустимые траектории и условия их возникновения.

При анализе траектории некорректного функционирования определяются необходимые изменения, дополняющие модель и устраняющие некорректные траектории в пространстве состояний. В данном примере, нарушения происходят при изменении уровня конфиденциальности и неизменности текущих доступов, что является известной проблемой классической модели. Для устранения данной проблемы существует несколько вариантов описанных в [22][23].

Для контроля событий, приводящих к нарушению свойств «Простой безопасности» и «*-правила», подсеть Петри, изображенная на рисунке 3 дополнена переходом и представлена на рисунке 9. Переход “AdditionalsChecks” осуществляет контроль изменений, содержащихся в запросе на корректность относительно существующих доступов.

Исследование модели для двух и трех видов доступа при неизменности сети Петри привело к обнаружению аналогичных траекторий некорректного функционирования. Изменение модели, представленное на рисунке 9, привело к их устранению.

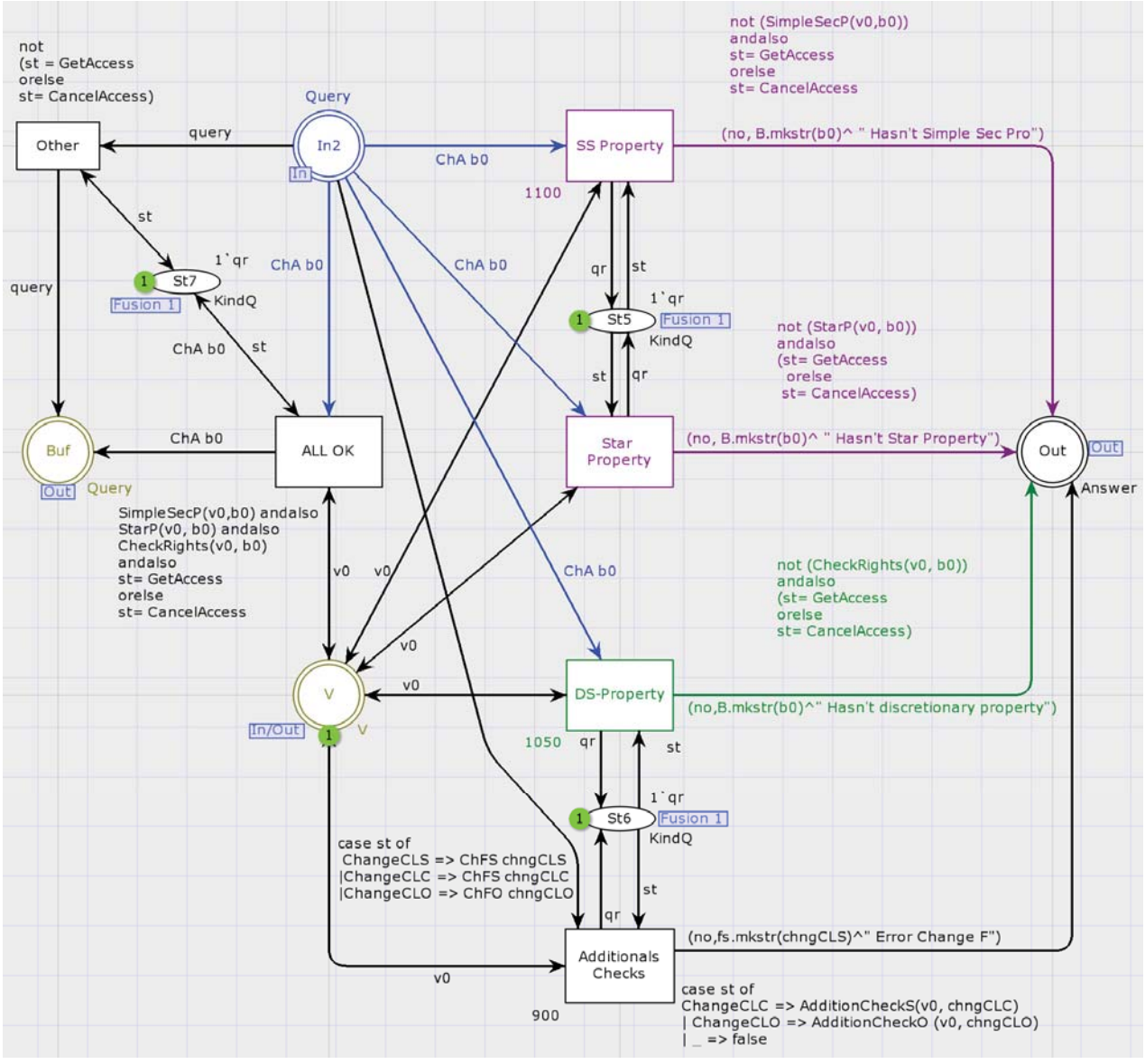


Рис. 9. Дополнения сети Петри для устранения некорректного функционирования

При построении пространства состояний для трех видов доступа было рассчитано 260713 узлов. Данное пространство состояний является частичным в соответствии с отчетом среды моделирования, что подтверждается исследованием. Из 260713 узлов конечными являлись 210428 узлов, а приводящими к некоренным состояниям 2500, что говорит о построении неполного пространства состояний. Построение неполного пространства является ограничением среды, для устранения которого, разрабатываются вспомогательные механизмы. Интеграция дополнительных средств анализа является одним из возможностей среды моделирования CPN Tools [24].

Одним из способов устранения комбинаторного взрыва является изменение уровня абстракции модели и уменьшении размерности начальной маркировки. Для примера возможностей моделирования, использованных в подходе, выбран подробный уровень абстракции с моделированием отдельных элементов множеств объектов и субъектов.

Помимо исследования полного пространства состояний [25] с последующей симуляцией в среде моделирования реализован механизм формальной верификации методом “Model Checking” с использованием ASK-CTL логики. Дополнение разработанного подхода использованием ASK-CTL логики и построение полного пространства состояния для сложных многоуровневых моделей является целью дальнейших исследований.

Заключение

Разработан подход к моделированию различных систем с использованием раскрашенных сетей Петри. На примере классической модели мандатного управления доступом продемонстрирован анализ информационной системы. Проведенный анализ позволил выявить известный недостаток модели Белла-Лаппадула, состоящий в возможности понизить уровень конфиденциальности без изменения множества текущих доступов, что подтверждает результативность предложенного подхода, и позволяет обоснованно сформировать компенсирующие меры для устранения обнаруженного некорректного функционирования.

Разработанная модель обладает структурной, логической и динамической эквивалентностью относительно исследуемого проекта информационной системы. Используемые в подходе методы и средства позволяют быстро вносить изменения в модель, обладают наглядностью и минимально достаточным набором примитивов, что облегчает процесс моделирования и изучения результатов.

Планируется адаптировать представленный подход для анализа более сложных свойств ИС, а также для автоматизации этапов поиска скрытых каналов. Для исследования больших (более 10 млн.) пространств состояний разрабатывается программное средство, дополняющее среду моделирования CPN Tools.

Литература

1. *Коршунов Г.И., Липатников В.А., Шевченко А.А., Малышев Б.Ю.* Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя// Информационно-управляющие системы. 2018. № 4. С. 61-72. doi:10.31799/1684-8853-2018-4-61-72

2. *Липатников В.А., Костарев С.В., Шевченко А.А.* Способ контроля уязвимостей информационно-вычислительных сетей критических инфраструктур // Перспективные направления развития отечественных информационных технологий : материалы IV межрегиональной научно-практической конференции, Севастополь, 18-22 сентября 2018 года / Севастопольский государственный университет; науч. ред. Б.В. Соколов. Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования "Севастопольский государственный университет", 2018. С. 255-256.

3. *Грушо А.А., Грушо Н.А., Тимонина Е.Е., Шоргин С.Я.* Архитектурные уязвимости распределенных информационно-вычислительных систем // Системы и средства информатики. 2016. Т. 26. № 3. С. 74-82. doi:10.14357/08696527160305

4. *Новиков В.А., Тихонов В.А.* Подход к моделированию перспективных информационных систем на основе аппарата цветных сетей Петри // Состояние и перспективы развития современной науки по направлению «Информационная безопасность» : Сборник статей III Всероссийской научно-технической конференции, Анапа, 21-22 апреля 2021 года. Анапа: Федеральное государственное автономное учреждение "Военный инновационный технополис "ЭРА", 2021. С. 129-138.

5. *Jensen, K., Kristensen, L.M., Wells, L.* Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. Int J Softw Tools Technol Transfer. 2007. №9, pp. 213-254. doi:10.1007/s10009-007-0038-x

6. *Wang J., Tepfenhart W.* Formal Methods in Computer Science (1st ed.). Chapman and Hall/CRC. 2019. doi:10.1201/9780429184185

7. *Петров А.Ю., Оленев В.Л.* Формальные методики исследования характеристик функционирования сетей // Аэрокосмическое приборостроение и эксплуатационные технологии : Сборник докладов Второй Международной научной конференции, Санкт-Петербург, 14-22 апреля 2021 года. Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2021. С. 309-316.

8. *Девянин П.Н., Кулямин В.В., Петренко А.К., Хорошилов А.В., Щепетков И.В.* Интеграция мандатного и ролевого управления доступом и мандатного контроля целостности в верифицированной иерархической модели безопасности операционной системы. Труды Института системного программирования РАН. 2020;32(1):7-26. doi:10.15514/ISPRAS-2020-32(1)-1

9. *Бирюков М.А., Зибров О.П., Саенко И.Б.* Способ реализации мандатной модели управления доступом на базе ролевой модели // Региональная информатика и информационная безопасность, Санкт-Петербург, 01-03 ноября 2017 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. С. 48-50.

10. *Окороков В.А., Лащук Д.Е.* Применение схемы многоуровневого доступа для организации защиты конфиденциальных данных // Вестник УрФО. Безопасность в информационной сфере. 2021. № 2(40). С. 22-30. doi:10.14529/secur210203

11. CPN Tools A tool for editing, simulating, and analyzing Colored Petri nets [Электронный ресурс] Режим доступа: https://cpntools.org/, (дата обращения 21.09.21).

12. *Liu Z., Liu J.* Formal Verification of Blockchain Smart Contract Based on Colored Petri Net Models // 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 2019, pp. 555-560. doi:10.1109/COMPSAC.2019.10265

13. *Лесняк Д.А., Матвеев С.А.* Моделирование комплекса средств защиты информации радиоканалов временными раскрашенными сетями Петри // СПбНТОРЭС: труды ежегодной НТК. – 2020. № 1(75). С. 127-130.

14. *Бацких А.В.* Имитационная модель процесса функционирования модифицированной подсистемы управления доступом системы защиты информации от несанкционированного доступа в программном окружении CPN TOOLS // Вестник ВИ МВД России. 2020. №3.

15. *Farah K., Chabir K., Abdelkrim M.N.* Colored Petri nets for modeling of networked control systems // 2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2019, pp. 226-230. doi:0.1109/STA.2019.8717215

16. *Jensen K., Kristensen L.M.* Hierarchical Coloured Petri Nets. In: Coloured Petri Nets. 2009. Springer, Berlin, Heidelberg. doi:10.1007/b95112_5

17. *Гаврилова А.С.* Сети Петри как инструмент моделирования параллельных процессов // Информационные системы и технологии в моделировании и управлении : IV Всероссийская научно-практическая конференция (с международным участием). Посвящается 75-летию Гуманитарно-педагогической академии (филиал) ФГАОУ ВО «КФУ им. В.И. Вернадского» в г. Ялте, Ялта, 21-23 мая 2019 года / отв. редактор К.А. Маковейчук. – Ялта: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2019. С. 69-73.

18. *Noori N.S.* Modeling the escalation/de-escalation of response operation levels in disaster response networks using hierarchical Colored Petri Nets (CPN) approach // Annual IEEE International Systems Conference (SysCon), 2018, pp. 1-8, doi:10.1109/SYSCON.2018.8369593.

19. *Blaga F., Blaga P., Vesselenyi T., Hule V., Indre C.* Modeling with hierarchical colored Petri nets. Case study // IOP Conference Series: Materials Science and Engineering. 2020. doi:10.1088/1757-899X/898/1/012017

20. *Jensen K., Kristensen L.M.* Formal Definition of State Spaces and Behavioural Properties. In: Coloured Petri Nets. 2009. Springer, Berlin, Heidelberg. doi:10.1007/b95112_9

21. *Болычев М.В., Мирошниченко Е.Л., Пасечник Р.М.* Алгоритм построения диаграммы достижимости модели состояния работоспособности информационной системы // Вопросы кибербезопасности. 2019. № 6(34). С. 79-91. doi:10.21681/2311-3456-2019-6-79-91

22. *Девянин П.Н., Кулямин В.В., Петренко А.К.* и др. Моделирование и верификация политик безопасности управления доступом в операционных системах. М.: Горячая линия-Телеком, 2019. 214 с.

23. *Kashmar N., Adda M, Atieh M., Ibrahim H.* Access Control Metamodel for Policy Specification and Enforcement: From Conception to Formalization, // Procedia Computer Science (2021), pp. 887-892. doi: 10.1016/j.procs.2021.03.111

24. *Карраскель Х.С., Моралес А., Виллаполь М.Е.* Prosega/CPN: расширение CPN Tools для автоматного анализа и верификации систем. Труды Института системного программирования РАН. 2018;30(4):107-128. doi:10.15514/ISPRAS-2018-30(4)-7

25. *Best E., Devillers R.* Characterisation of the state spaces of marked graph Petri nets // Information and Computation. 2017, vol. 253, Part 3, pp. 399-410. doi: doi.org/10.1016/j.ic.2016.06.006

VERIFICATION OF ACCESS CONTROL SYSTEMS BASED ON MODELING WITH COLORED PETRI NETS

VALERY A. TIKHONOV
St. Petersburg, Russia v.tihonov@ao-trk.ru

VLADIMIR A. NOVIKOV
St. Petersburg, Russia, v.novikov@ao-trk.ru

KEYWORDS: *formal verification, information security, colored Petri net, modelling, compliance assessment.*

ABSTRACT

Introduction: the complexity of the information systems (IS) being developed increases the requirements for the error-free design of the access control system and increases the likelihood of the presence and impact of vulnerabilities on the state of information security. Formal verification of the IS project at the development stage allows minimizing the appearance of architectural vulnerabilities. Changes carried out by regulators in the field of certification of information security means actualizing issues related to the development and analysis of formal models. **Purpose:** development of an approach to the construction and formal verification of models that has an intuitively, completeness presentation and effective analysis. **Methods:** construction of models by the mathematical apparatus of colored Petri nets in the CPN Tools modeling environment with the subsequent study of the properties of the net. **Results:** an approach has been developed that has structural, logical and dynamic completeness. The clarity of the models developed using the presented approach reduces the time for detecting incorrect functioning and developing compensatory measures with the subsequent confirmation of their effectiveness. The analyze of the state space showed the need to supplement the modeling environment for the complete construction of the state space in the case of complex models and a large number of markers during the initial marking of the Petri net. **Practical relevance:** the developed approach is proposed to be used for formal verification of access control models and filtering information flows in the certification procedure for information security tools. The versatility and simplicity of the approach allows you to implement the formal verification procedure in the development stages of various kinds of systems. **Development prospects:** development of additional software that allows building a complete state space for complex models, as well as complementing the method with approaches using ASK-CTL logic.

REFERENCES

1. G.I. Korshunov, V.A. Lipatnikov, A.A. Shevchenko, B.Y. Malyshev (2018). Adaptive Management of Information Network Protection with Analysis of Intruder's Actions. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], no. 4, pp. 61-72 (In Russian). doi:10.31799/1684-8853-2018-4-61-72

2. V. A. Lipatnikov, S.V. Kostarev, A. A. Shevchenko (2018). Method of controlling sensibilities of computer networks of critical infrastructure. *Advanced national information systems and technologies Materials of IV interregional scientific-practical conference Sevastopol*, September 18-22, pp. 255-256. (In Russian)

3. A.A. Grusho, H.A. Grusho, E.E. Timonina, S.Ya. Shorgin. (2016). Architectural vulnerabilities of distributed information systems. Systems and means of informatics. Мщдю. 26. No. 3, pp. 74-82. doi:10.14357/08696527160305 (In Russian)

4. V.A. Novikov, V.A. Tikhonov (2021).An approach to modeling advanced information systems based on the apparatus of color Petri nets. *Sostoyanie i perspektivy razvitiya sovremennoy nauki po napravleniyu "Informatsionnaya bezopasnost'" : Sbornik statey III Vserossiyskoy nauchno-tekhnicheskoy konferentsii*, Anapa, 21-22 april 2021. Anapa: Federal'noe gosudarstvennoe avtonomnoe uchrezhdenie "Voennyy innovatsionnyy tekhnopolis "ERA", pp. 129-138. (In Russian)

5. K. Jensen, L.M. Kristensen, L. Wells. (2007). Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. *Int J Softw Tools Technol Transfer. No.* 9, pp. 213-254. doi:10.1007/s10009-007-0038-x

6. J. Wang, W. Tepfenhart (2019). Formal Methods in Computer Science (1st ed.). Chapman and Hall/CRC. doi:10.1201/9780429184185

7. A.U. Petrov, V.L. Olenev. (2021). Formal methods of research the characteristics of network functioning. Ajerokosmicheskoe priborostroenie i jekspluatacionnye tehnologii : Sbornik dokladov Vtoroj Mezhdunarodnoj nauchnoj konferencii, Sankt-Peterburg, 14-22 april 2021. Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet ajerokosmicheskogo priborostroenija, pp. 309-316.

8. P.N. Devyanin, V.V. Kulyamin, A.K. Petrenko, A.V. Khoroshilov, I.V. Shchepetkov. (2020). Integrating RBAC, MIC, and MLS in Verified Hierarchical Security Model for Operating System. *Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS).* No. 32(1), pp. 7-26. (In Russian). doi:10.15514/ISPRAS-2020-32(1)-1

9. M. Biryukov, O. Zibrov, I. Saenko. (2017). The method of mandatory access control implementation by role-based access control facilities. *Regional'naja informatika i informacionnaja bezopasnost'*, Sankt-Peterburg, 01-03 november 2017. Sankt-Peterburg: Sankt-Peterburgskoe Obshhestvo informatiki, vychislitel'noj tehniki, sistem svjazi i upravlenija, pp. 48-50. (In Russian)

10. V.A. Okorokov, D.E. Laschuk. (2021). Application of a multi-level access scheme for protecting confidential data. *Bulletin of the Ural Federal District. Security in the Information Sphere*. No. 2(40), pp. 22-30. doi:10.14529/secur210203

11. CPN Tools A tool for editing, simulating, and analyzing Colored Petri nets.

12. Z. Liu and J. Liu. (2019). Formal Verification of Blockchain Smart Contract Based on Colored Petri Net Models," *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, pp. 555-560, doi:10.1109/COMPSAC.2019.10265

13. D.A. Lesnyak, S.A. Matveev. (2020). Modelirovanie kompleksa sredstv zashchity informatsii radiokanalov vremennymi raskrashennymi setyami Petri. *SPbNTORES: trudy ezhegodnoy NTK*. No. 1(75), pp. 127-130. (In Russian)

14. A.V. Batskikh (2020). Simulation model of the functioning of the modified access control subsystem of the information protection system against unauthorized access in the cpn tools software environment. *Vestnik of voronezh institute of the ministry of interior of Russia*. No.3. (In Russian)

15. K. Farah, K. Chabir and M.N. Abdelkrim (2019). Colored Petri nets for modeling of networked control systems. 2019 *19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, pp. 226-230, doi:0.1109/STA.2019.8717215

16. K. Jensen, L.M. Kristensen (2009). Hierarchical Coloured Petri Nets. In: Coloured Petri Nets. Springer, Berlin, Heidelberg. doi:10.1007/b95112_5

17. A. S. Gavrilova (2019). Seti Petri kak instrument modelirovanija parallel'nyh processov. *Informacionnye sistemy i tehnologii v modelirovanii i upravlenii : IV Vserossijskaja nauchno-prakticheskaja konferencija (s mezhdunarodnym uchastiem)*. Posvjashhaetsja 75-letiju Gumanitarno-pedagogicheskoj akademii (filial) FGAOU VO "KFU im. V.I. Vernadskogo" v g. Jalte, Jalta, 21-23 May 2019, editor K.A. Makovejchuk. Jalta: Obshhestvo s ogranichennoj otvetstvennost'ju "Izdatel'stvo Tipografija "Arial", pp. 69-73. (In Russian)

18. Noori N.S. (2018). Modeling the escalation/de-escalation of response operation levels in disaster response networks using hierarchical Colored Petri Nets (CPN) approach. *Annual IEEE International Systems Conference (SysCon)*, pp. 1-8, doi:0.1109/SYSCON.2018.8369593

19. F. Blaga, P. Blaga, T. Vesselenyi, V. Hule, C. Indre (2020). Modeling with hierarchical colored Petri nets. Case study. *IOP Conference Series: Materials Science and Engineering*. doi:10.1088/1757-899X/898/1/012017

20. K. Jensen, L.M. Kristensen (2009). Formal Definition of State Spaces and Behavioural Properties. In: Coloured Petri Nets. Springer, Berlin, Heidelberg. doi:10.1007/b95112_9

21. Maxim Bolychev, Evgeniy Miroshnichenko, Rodion Pasechnik (2019). Algorithm for Creating the Model of Attainability of Information System Operability Status Model. *Voprosy kiberbezopasnosti*, pp. 79-91. 10.21681/2311-3456-2019-6-79-91 (In Russian)

22. P.N. Devyanin, V.V. Kulyamin, A.K. Petrenko ets. (2019). Modelirovanie i verifikatsiya politik bezopasnosti upravleniya dostupom v operatsionnykh sistemakh. Moscow: Goryachaya liniya-Telekom, 214 p.

23. Nadine Kashmar, Mehdi Adda, Mirna Atieh, Hussein Ibrahim (2021). Access Control Metamodel for Policy Specification and Enforcement: From Conception to Formalization. *Procedia Computer Science*, pp. 887-892. doi:10.1016/j.procs.2021.03.111

24. Kh.C. Carrasquel, A. Morales, M.E. Villapol. (2018). Prosega/CPN: An Extension of CPN Tools for Automata-based Analysis and System Verification. *Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS).* No. 30(4), pp. 107-128. doi:10.15514/ISPRAS-2018-30(4)-7

25. Eike Best, Raymond Devillers (2017). Characterisation of the state spaces of marked graph Petri nets. *Information and Computation*, vol. 253, Part 3, pp. 399-410 .doi:10.1016/j.ic.2016.06.006

INFORMATION ABOUT AUTHORS:

Tikhonov V.A., engineer researcher JSC "Radiomonitoring technologies"

Novikov V.A., PhD. Head of the test center JSC "Radiomonitoring technologies"

For citation: Tikhonov V.A., Novikov V.A. Verification of access control systems based on modeling with colored Petri nets // H&ES Reserch. 2021. Vol. 13. No. No 6. P. 50-59. doi: 10.36724/2409-5419-2021-13-6-50-59 (In Rus)