А.В. Царегородцев, А.К. Качко

ОДИН ИЗ ПОДХОДОВ К МОДЕЛИРОВАНИЮ МАРШРУТА РАСПРЕДЕЛЕНИЯ ОБРАБОТКИ КРИТИЧНЫХ ДАННЫХ В ГИБРИДНОЙ СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Аннотация: *Использование облачных вычислений при построении ИТ-инфраструктуры организации подразумевает отказ организации от прямого контроля над аспектами безопасности. Возникает необходимость в решении задачи обеспечения конфиденциальности данных при проектировании архитектуры, основанной на технологии облачных вычислений. Предлагаемый подход к моделированию процесса обработки данных с помощью сетей Петри на основании требований политики безопасности организации позволяет получить важную информацию о структуре многоуровневой системы управления доступом в гибридной облачной среде, что в конечном итоге позволит проследить динамическое поведение обработки критических данных в моделируемой системе.*

Ключевые слова: *модели безопасности компьютерных систем, облачные вычисления, публичное облако, частное облако, гибридное облако, требования безопасности, конфиденциальность данных, моделирование.*

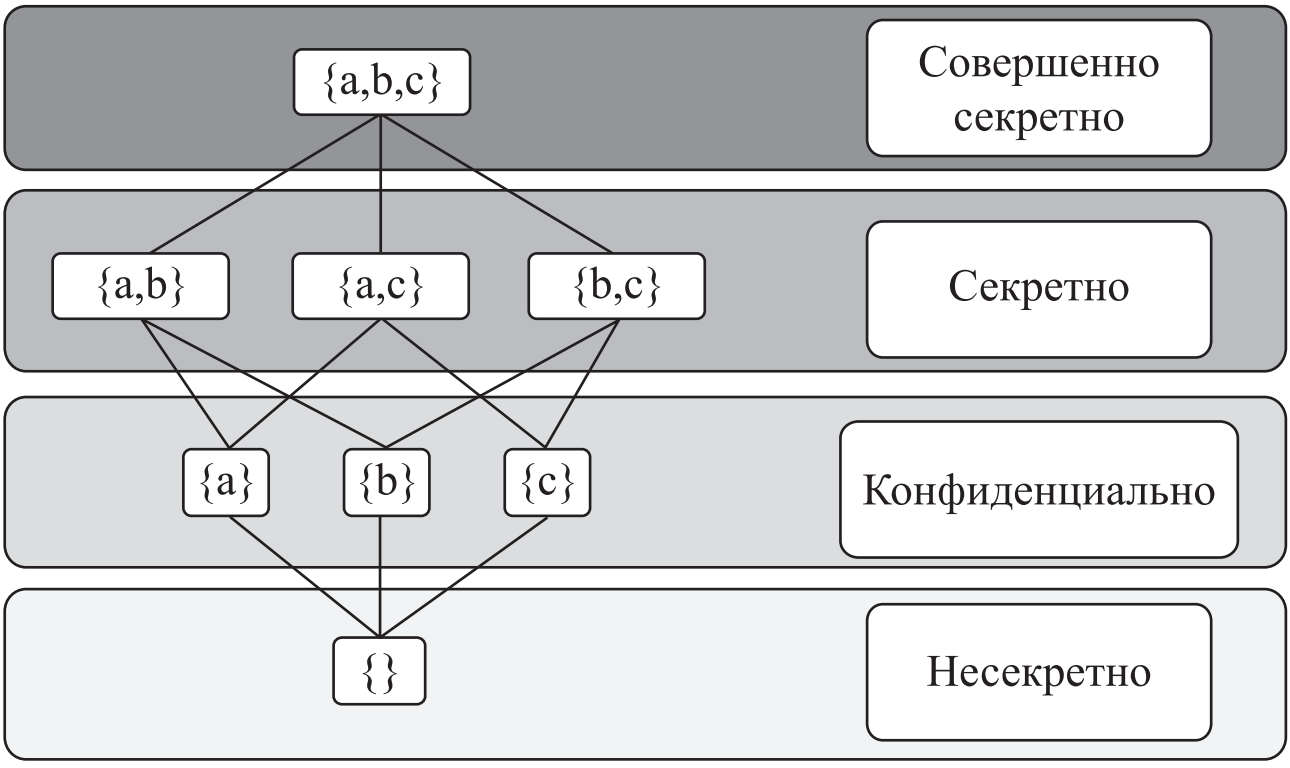
Введение

Принимая во внимание парадигму облачных вычислений, организация отказывается от прямого контроля над многими аспектами безопасности и, тем самым, создаёт беспрецедентный уровень доверия облачному провайдеру [2]. Преимущества облачных вычислений могут позволить существенно сократить сроки и издержки на разработку систем для федеральных агентств и государственных организаций. Особую актуальность принимает гибридная модель развёртывания облачных сервисов, которая подразумевает обработку критичных данных в частной среде облачных вычислений, которая находится под полным контролем организации. Но многие из функций, которые делают привлекательными облачные вычисления, могут вступать в противоречие с традиционными моделями обеспечения информационной безопасности. При анализе сложных бизнес процессов очень трудно определить факт соответствия текущих полномочий субъекта к объекту доступа с соответствующим уровнем секретности. В связи с этим возникает необходимость в разработке системного подхода, позволяющего смоделировать процесс обработки данных в разрезе двух потоков: потока управления и потока обработки критичных данных. Моделирование предполагается осуществлять на основе сетей Петри с целью определения соответствия с утверждённой политикой безопасности организации в условиях гибридной среды облачных вычислений.

1. Многоуровневая политика безопасности среды облачных вычислений

Многоуровневая политика безопасности имеет давнюю традицию в военной среде и является важным критерием оценки защищенности вычислительных систем для классов A и B (TCSEC, “Оранжевая книга”). В качестве примера приведём два варианта классификации секретности данных на основе диаграммы Хассе (рисунок 1) [3]. Первый вариант применяется для классификации информации военного характера, уровни секретности расположены в линейной зависимости. Второй вариант – более сложный и представляет собой все подмножества множества $\rho(\{a,b,c\})$. Важно, что $\{a,b\} \not\subseteq \{b,c\}$ и $\{b,c\} \not\subseteq \{a,b\}$, поэтому их нельзя упорядочить между собой. Для первого варианта наивысшим уровнем является уровень «совершенно секретно», что соот-

ветствует множеству {a,b,c}, а наименьшим – «несекретно» {}.



Вариант 2 Вариант 1

Рис. 1. Решётка безопасности

Политика безопасности организации – это одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности. Определим в рамках политики безопасности множество субъектов безопасности T и множество объектов O, функцию безопасности f, которая для каждого объекта и субъекта определяет принадлежность уровня безопасности $l \in L$, где $(L, \leq)$ структура вида $f: S \cup O \rightarrow L$ [4]. Теория сетей Петри делает возможным моделирование системы математическим представлением её в виде сети Петри.

2. Моделирование обработки данных в среде облачных вычислений

Приведём ключевые факторы, которые подтверждают эффективность использования сетей Петри для моделирования обработки данных в среде облачных вычислений:

1. сети Петри изначально разрабатывались для моделирования систем, которые содержат взаимодействующие параллельные компоненты;
2. сети Петри позволяют описать причинные связи между событиями;
3. действия одной компоненты могут производиться одновременно с действиями других компонент.

Граф сети Петри обладает двумя типами узлов: «○» является позицией, а планка «|»– переходом. Ориентированные дуги (стрелки) соединяют позиции и переходы, при этом некоторые дуги направлены от позиций к переходам, а другие – от переходов к позициям. Дуга, направленная от позиции к переходу, определяет позицию, которая является входом перехода. Выходная позиция указывается дугой от перехода к позиции. Действиям компонент системы присущи совмещенность и параллелизм. Действия одной компоненты могут производиться одновременно с действиями других компонент. Пересылка информации от одной компоненты к другой требует,

чтобы действия включенных в обмен компонент были во время взаимодействия синхронизированы [1].

Проведём анализ распределения потока критичных данных в рамках среды облачных вычислений на основании предложенных выкладок. Действия над данными отобразим в виде переходов сети Петри таким образом, что выполнение задачи связано с осуществлением перехода, вследствие которого появляется маркировка сети, что определяет текущее состояние процесса обработки данных.

Предполагается использовать элементы данных и их позиции для определения в сети Петри двух потоков [5]:

- управляющий поток;
- поток данных.

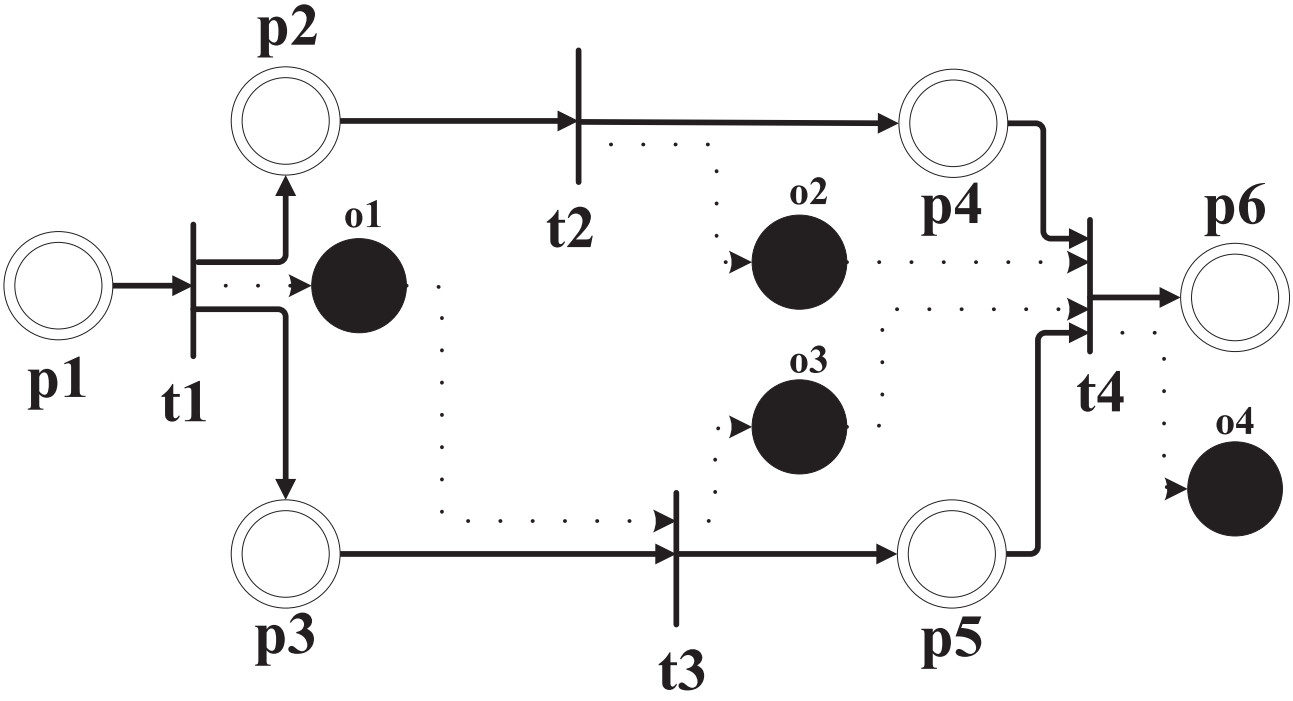
На рисунке 2 данные $o_1,\ldots, o_5$ и отношения между ними (стрелочки) изображены в виде пунктирной линии (поток данных). Управляющий поток показан в виде сплошной линии (данные типа $p_1,\ldots, p_5$ и их переходы). Выполнение задачи требует наличия маркёра, передаваемого с данными, на входной позиции t и приводит к созданию маркёра в выходной позиции t. То есть при выполнении задачи t доступ на чтение данных определяется наличием входного маркера, доступ на запись данных – выходного маркера. Рисунок 2 отражает полное выполнение процесса обработки данных, то есть конечное состояние процесса является *достижимым*.

Рассмотрим пример, когда облачный сервис на вход получает данные o_1, o_3 и производит данные o_4. В этом случае субъект политики безопасности должен иметь доступ на чтение данных o_1 и o_3 и доступ на запись данных o_4. Тогда субъект T должен иметь возможность читать все данные с маркером $\bullet\, t$ и записывать данные с маркером . Если для субъекта T и элементов в области $\bullet\, t \cup t\, \bullet$ присвоены соответствующие уровни доступа в соответствие с требованиями политики безопасности организации. Выполнение процесса обработки данных должно контролироваться управляющим элементом, который создаёт различные варианты развёртывания процесса обработки данных. Определение, является ли процесс полностью выполнимым, то есть конечная маркировка достижима из стартовой маркировки, представляет собой нетривиальную задачу, но может быть решена с помощью различных аналитик.

Определим субъекты безопасности, как $T = \{t_1, t_2, t_3\}$, элементы данных $O = \{o_1, o_2, o_3, o_4\}$, элементы управления $P = \{p_1, p_2, p_3, p_4, p_5, p_6\}$, задачи/переходы $T = \{t_1, t_2, t_3, t_4\}$, для начальной позиции $M(p_1) = 1$, другие маркировки для неё равны 0.

На рисунке 3 изображено 6 состояний процесса обработки данных в виде узлов. Каждое состояние характеризуется двумя столбцами: первый из столбцов (p) отражает состояние потока управления, второй (o) – состояние потока данных. Например, узел

Рис. 2. Процесс обработки критичных данных, изображенный в виде сети Петри



V имеет маркеры для данных $\{p_4,p_5\}$ (левый столбец узла *V*), $\{o_2,o_3\}$ (правый столбец узла *V*).

Принципы построения сети Петри по требованиям безопасности, представим в виде следующих положений.

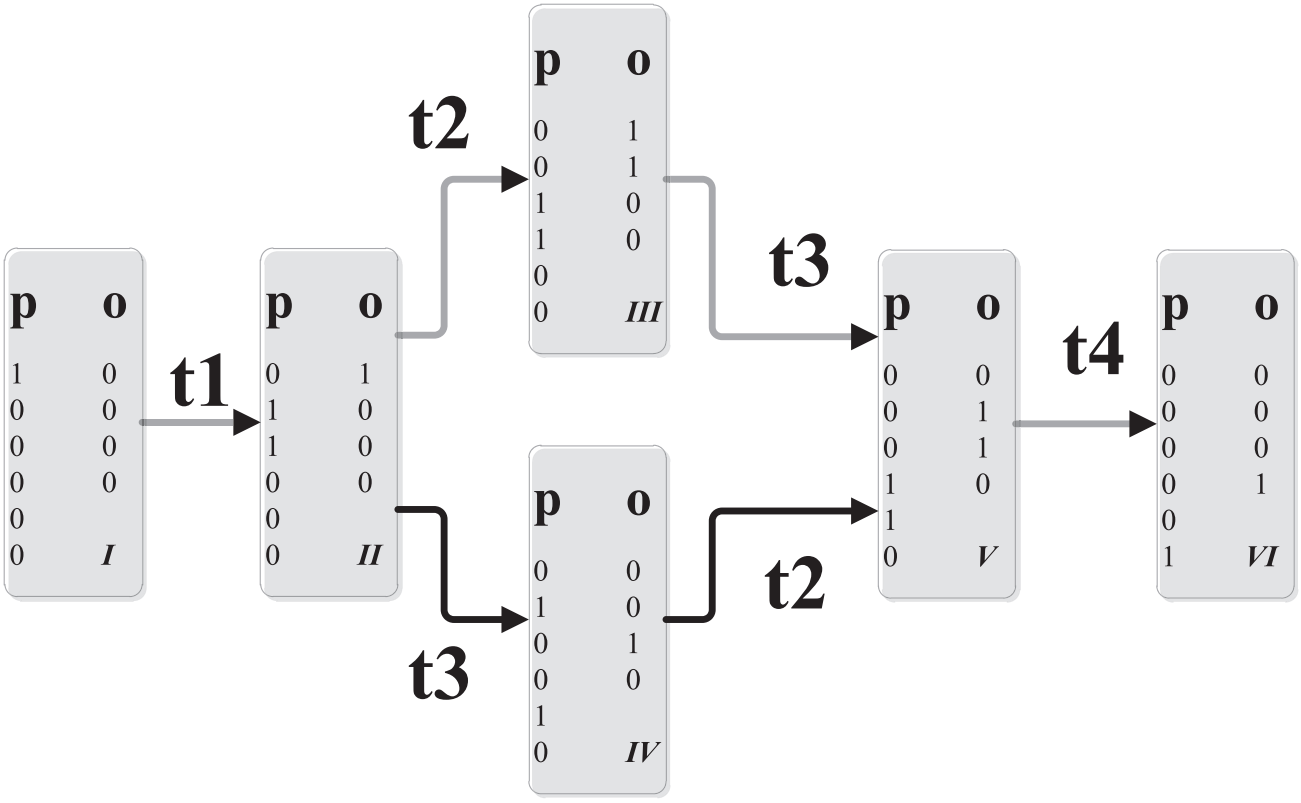


Рис. 3. Состояния процесса обработки данных

Примем во внимание требования политики безопасности «*» и «*ss*» классической модели доступа Белла-ЛаПадула [6]. Для наглядности примера определим шкалу уровней информационной безопасности, состоящую из двух уровней: «Секретно» и «Несекретно».

Присвоим уровни безопасности для субъектов рассматриваемого процесса, таким образом, что все задачи будут наследовать полномочия роли, под которыми они выполняются (таблица 1)

• Если субъект (облачный сервис) имеет высокий уровень доступа, то:

– разрешается совершать переход от узла *N* к узлу *M*, в результате которого происходит запись данных с высоким уровнем секретности;

– разрешается совершать переход от узла *N* к узлу *M*, в результате которого происходит чтение данных высокого или низкого уровней секретности.

– запрещается совершать переход от узла *N* к узлу *M*, в результате которого происходит запись данных низкого уровня секретности.

Таблица 1

Уровни доступа облачных сервисов

Функция безопасности	**Уровень ИБ**
$f(t_1)=f(t_2)=f(t_4)$	Низкий (Несекретно)
$f(t_3)$	Высокий (Секретно)

• Если субъект (облачный сервис) имеет низкий уровень безопасности, то:

– разрешается совершать переход от узла N к узлу M, в результате которого происходит запись данных с высоким или низким уровнем секретности;

– разрешается совершать переход от узла N к узлу M, в результате которого происходит чтение данных низкого уровня секретности.

– запрещается совершать переход от узла N к узлу M, в результате которого происходит чтение данных высокого уровня секретности.

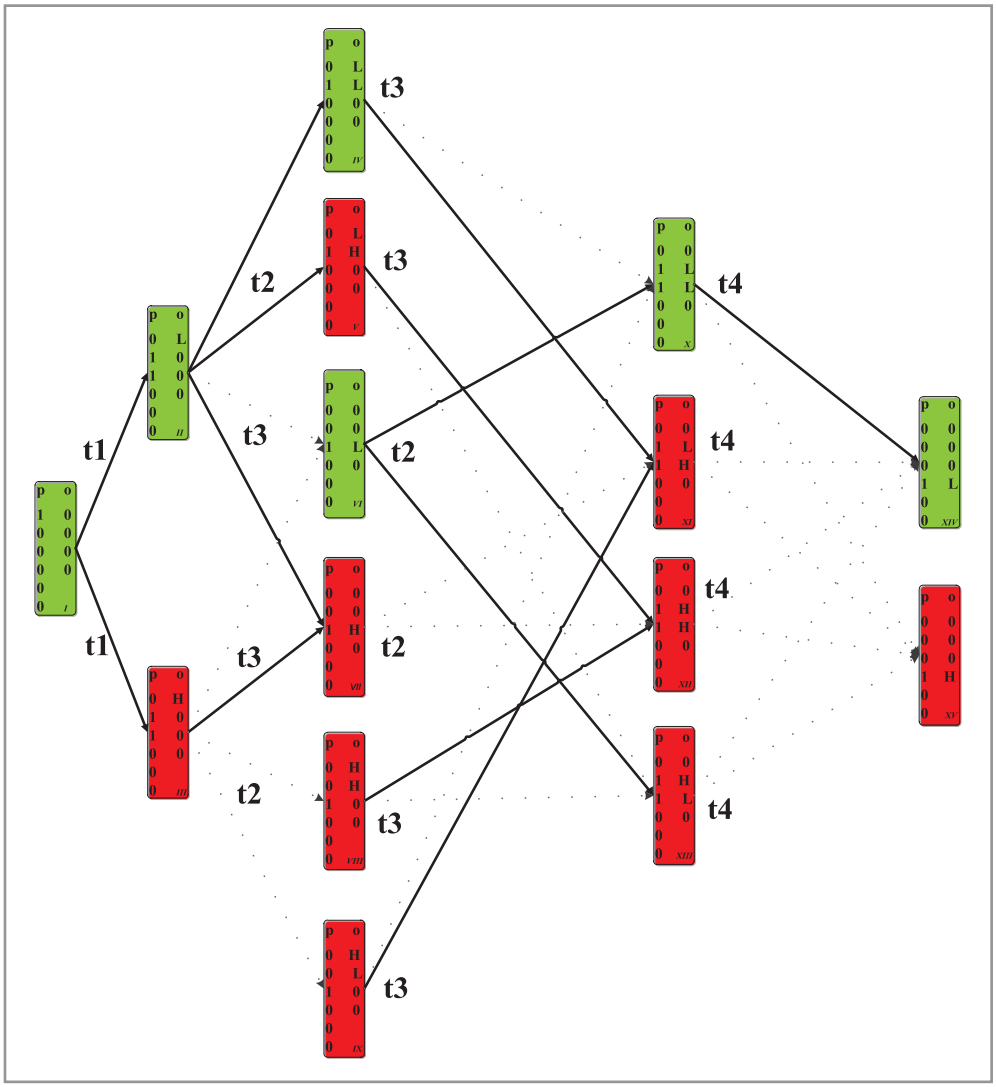
В результате применения данных принципов формируется граф, который учитывает присвоенные уровни доступа всех субъектов рассматриваемого процесса и в зависимости от полномочий принимается решение о маркировке данных (рисунок 4). Рисунок 4 состоит из 15 узлов, которые показывают возможные маркировки обрабатываемых данных в сети Петри. Значения первого столбца показывают маркировку потока управления $p_1, p_2, p_3, p_4, p_5, p_6$, значения второго – маркировку потока данных с соответствующими уровнями секретности для o_1, o_2, o_3, o_4. Например, узел *XI* имеет две управляющие метки данных p_2, p_3 метку данных с высоким уровнем безопасности o_3, метку данных с низким уровнем безопасности o_2.

Для наглядности и лучшего восприятия сети Петри предлагается использовать различные цвета для каждого узла.

Узлы, в рамках которых происходит обработка критичных данных, раскрашены в красный цвет и соответствуют компоненту частной среды облачных вычислений.

Узлы, в рамках которых происходит обработки несекретных данных, раскрашены в зеленый цвет. Данные узлы можно развернуть на общедоступной среде облачных вычислений, которая имеет более низкую стоимость, чем частная.

Рис. 4. Сеть Петри с присвоенными уровнями секретности для данных и сервиса



Построенная сеть Петри имеет два вида управляющих стрелок:

1. *сплошная линия* используется для описания валидной маркировки, где отсутствуют нарушения требования «*» и «ss»;
2. *пунктирная линия* описывает маркировку данных, нарушающую одно из требований политики безопасности.

Выборочно приведём примеры нарушения политики безопасности построенного графа (наличие пунктирной линии) на рисунке 4.

- Переход от состояния *II* к состоянию *VI* нарушает требование «*ss*» (принцип №3), то есть запрещается совершать переход от узла *N* к узлу *M*, в результате которого субъектом с высоким уровнем безопасности (t_3) инициируется запись данных низкого уровня секретности (o_3).
- Переход из состояния *XII* в состояние *XV* нарушает требование «*» (принцип №6), то есть запрет чтения информации с высоким уровнем секретности o_2, o_3 субъектом с более низким уровнем безопасности (t_4).
- Если в модель ввести трехуровневую шкалу секретности, то возможен случай, когда субъект со средним уровнем безопасности запросит доступ на чтение к данным с высоким уровнем и инициирует запись объекта с низким уровнем секретности. Данные действия нарушат оба требования политики безопасности, построенной на требованиях Белла-ЛаПадула.

Детальный анализ рисунка 4 показывает, что не существует маршрута, который полностью удовлетворяет требованиям безопасности и делает возможным переход из состояния *I* в состояние *XIV* или *XV*. Для данного примера требования «ss» и «*» оказались невыполнимыми.

Можно рассмотреть разные варианты решения полученной проблемы.

Адаптировать текущую сеть Петри и включить в неё новые элементы. Введение в модель демилитаризованных зон, роль которых могут выполнять частные облака, позволит построить маршрут, выполнение которого выполнит основное требование *достижимости* сети Петри. Частное облако должно быть развёрнуто для обработки состояний, в которых в результате переходов (выполнения заданий) создаются критичные данные (с высоким уровнем секретности).

Изменить, если возможно, решетку безопасности для облачных сервисов и данных с последующим изменением политики безопасности, например:

Заключение

Предлагаемый подход к моделированию процесса обработки данных с помощью сетей Петри на основании требований политики безопасности организации позволяет получить важную информацию о структуре многоуровневой системы управления доступом в гибридной облачной среде, что в конечном итоге позволит проследить динамическое поведение обработки критических данных в моделируемой системе. Эта информация будет полезна для следующих задач.

1. Оценка стоимости построения компонентов гибридной среды облачных вычислений.
2. Выбор оптимального варианта распределения обработки критичных данных между общедоступным и частным облаком.
3. Проведение оценки риска для каждого компонента и выработке предложений усовершенствованию и изменению выбранной архитектуре.

При рассмотрении более сложных случаев если заранее известны веса нарушений и их возможные последствия (увеличение уровней безопасности, количества позиций и субъектов в сети) рекомендуется поиск минимального (оптимального) маршрута с помощью построенного графа. Для решения задач такого рода широкое распространение получил метод ПЕРТ (метод оценки и пересмотра планов), применение которого можно рассмотреть для продолжения научного исследования над данной проблематикой.

Библиография:

1. Питерсон Дж. Теория сетей Петри и моделирование систем. – М.:МИР, 1981. – 263 с.
2. National Institute of Standards and Technology (NIST) Definition of Cloud Computing, http://csrc.nist.gov/groups/SNS/cloud-computing/
3. R.L. Trope, E.M. Power, V.I. Polley and B.C.Morley. «A Coherent Strategy for Data Security through Data Governance». IEEE Security & Privacy, vol. 5, no. 3, pp. 32-39, May/Jun. 2007.

Функция безопасности	Уровень ИБ
$f(o_1) = f(o_3) = f(o_4) = f(o_5)$	Высокий
$f(o_2)$	Низкий

4. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7. 2002. 1084 p.
5. R. Accorsi, C. Wonnemann. «Auditing Workflow Execution against Dataflow Policies» In Proc. BIS, 2010, pp. 207-217.
6. Bell, D. E. and LaPadula, L. J.: Secure Computer System: Unified Exposition and Multics Interpretation, Tech report ESD-TR-75-306, Mitre Corp, Bedford, Ma. (1976).

References (transliteration):

1. Piterson Dzh. Teoriya setey Petri i modelirovanie sistem. – M.:MIR, 1981. – 263 s.
2. National Institute of Standards and Technology (NIST) Definition of Cloud Computing, http://csrc.nist.gov/groups/SNS/cloud-computing/
3. R.L. Trope, E.M. Power, V.I. Polley and B.C.Morley. «A Coherent Strategy for Data Security through Data Governance». IEEE Security & Privacy, vol. 5, no. 3, pp. 32-39, May/Jun. 2007.
4. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7. 2002. 1084 p.
5. R. Accorsi, C. Wonnemann. «Auditing Workflow Execution against Dataflow Policies» In Proc. BIS, 2010, pp. 207-217.
6. Bell, D. E. and LaPadula, L. J.: Secure Computer System: Unified Exposition and Multics Interpretation, Tech report ESD-TR-75-306, Mitre Corp, Bedford, Ma. (1976).

