УДК 004.056.53

# ЛОГИКО-ЯЗЫКОВЫЕ СРЕДСТВА ДЛЯ ОПИСАНИЯ МОДЕЛИ УПРАВЛЕНИЯ РАЗГРАНИЧЕНИЯ ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

***© 2022 А. Б. Сизоненко, А. О. Титарев, И. С. Рудь***

*Рассмотрены существующие логико-языкового описания систем управления разграничением доступа (СУРД), рассмотрены их положительные и отрицательные стороны. Предложен новый метод описания СУРД с помощью языка JSON в целях наиболее точного анализа нагрузки на администраторов (операторов) безопасности информации информационных систем, а также временных затрат необходимых для проведения операций по разграничению доступа в информационных системах.*

*Ключевые слова: эргатические системы, социотехнические системы, логико-языковые средства, система защиты информации, пользователи, управление правами доступа, средства защиты информации, полномочия, система массового обслуживания.*

В настоящее время в целях защиты информации в информационных системах (ИС) создаются комплексные и сложно организованные системы управления разграничения прав доступа пользователей к защищаемым информационным ресурсам (далее – УПД).

В связи с ростом и развитием ИС развивается сложность и систем УПД. В современных системах защиты информации обслуживается огромное количество пользователей, защищаемых информационных ресурсов (ЗИР) и различных правил доступа к этим. Все это порождает большое множество связей вида [пользователь]х[право доступа]х[ЗИР].

Пользователь и ответственный за обеспечение защиты информации являются людьми, это приводит к тому, что система УПД является эргатической системой. В данных системах, так как их особенностью являются социально-психологические аспекты, одной из основных проблем в защите информации является человеческий фактор. По классификации систем «человек-машина» в части ИС чаще всего выделяются две группы: 1) управляющие – ответственные по защите информации (ответственные по ЗИ); 2) операторы – непосредственно сами пользователи информационных систем (далее в тексте для краткости и ответственные за ЗИ, и операторы будут излагаться как операторы).

Существует множество моделей, описывающих системы защиты информации в части управления правами доступа, однако, ни одна из них не является универсальной, и каждая из них предназначена для рассмотрения системы с какой-то одной стороны. Модели, описывающие систему ЗИ УПД, демонстрирующую сложность ее администрирования, в настоящее время найти проблематично. Построить такую модель и описать ее характеристики сложно, но чрезвычайно важно. Для описания подобной специфической модели необходимо использовать удобный для этого логический язык.

Рассмотрим несколько известных подходов описания для формализации систем УПД.

Андреев О. О. предлагает использовать для построения моделей УПД логико-языковое средство eXtended Access Control Language (XACML) [2]. Этот язык, являющийся декларативным, основанным на XML (eXtensible Markup Language) языком описания моделей логического разграничения доступа, стандартизован международной организацией OASIS (Organization for the advancement of structured information standards) [1]. В настоящее время имеется большое количество теоретических исследований XACML, ведутся работы по практическому внедрению механизмов, основанных на этом языке, в существующие системы [3]. Широкое распространение языка

Сизоненко А.Б. – Краснодарское высшее военное училище, доктор технических наук, доцент.
Титарев Александр Олегович – Краснодарское высшее военное училище, слушатель магистратуры, e-mail: mr.titarev@mail.ru.
Рудь И.С. – Краснодарское высшее военное училище, слушатель магистратуры а, e-mail: science.80@mail.ru.

XACML обусловлено богатством выразительных средств, позволяющих задавать широкий спектр моделей разграничения доступа, в том числе такие распространенные модели, как дискреционная и многоуровневая. Еще одним преимуществом данного языка, обеспечившим его популярность, в том числе в научных кругах, является декларативность, позволяющая упростить анализ свойств моделей разграничения доступа, заданных с помощью XACML [4, 5].

Данный язык отлично подходит для описания таких элементов системы УПД как [пользователь]x[право доступа]x[ЗИР]. Однако, не подходит для описания сложности администрирования системы УПД.

Девянин П. Н. [5] описывает общее состояние системы G, состоящей из множества учетных записей пользователей, прав доступа к сущностям, сущностей, функции административных прав доступа к ролям административных ролей, иерархии ролей, сущностей, субъект-сессий. При этом учитывается множество всех возможностей состояний и правил перехода из состояния в состояние. Данное описание предназначено для верификации политик безопасности управления доступом в операционных системах.

Указанные логико-языковые средства не удобно использовать для описания УПД как процесса с точки зрения анализа динамики нагрузи на администратора безопасности. Так как в этих целях необходимо добавлять дополнительные параметры к элементам УПД, а также для наибольшей наглядности предлагается использовать зык JSON.

JSON (JavaScript Object Notation) – текстовый формат обмена данными, основанный на JavaScript. Как и многие другие текстовые форматы, JSON легко читается людьми. Формат JSON был разработан Дугласом Крокфордом [6].

Несмотря на происхождение от JavaScript (точнее, от подмножества языка стандарта ECMA-262 1999 года), формат считается независимым от языка и может использоваться практически с любым языком программирования. Для многих языков существует готовый код для создания и обработки данных в формате JSON. За счёт своей лаконичности по сравнению с XML формат JSON может быть более подходящим для сериализации сложных структур.

При рассмотрении нагрузки администратора безопасности одним из важных аспектов является время, затраченное на проведение тех или иных операций. При этом нужно учитывать то, что время отработки запроса зависит от компетенции оператора, а также сложности операции.

Рассмотрим пример применения языка JSON для описания системы УПД.

Предположим, что у нас есть некая ИС в которой количество пользователей равно 58, количество защищаемых ресурсов – 3 каталога (далее – папки), разновидность прав – 2 (чтение, запись). Обычно, говорят, что если на настройку прав одному пользователю на одну папку в среднем равно 4 минуты, то значит для 58 пользователей на 3 папки будет 58·3·4 = 696 минут.

Однако, как правило, тут не учитывается, что из-за разной размерности каждой папки или сложности пути к ней, или других особенностей на каждую папку может быть потрачено разное количество времени. Также разное количество времени может быть потрачено на разные права доступа (предположим, что для предоставления права на запись нужно проверять принадлежность к соответствующему структурному подразделению), или на разного пользователя (например, если пользователь уже создан, то это одно время, если нужно сначала создавать пользователя и потом назначать ему права – это уже другое время).

Здесь нужно подходить дифференцированно.

Опишем эту ИС в JSON:

```
IS1:
{
   users: 58;
elements: 3;
   rules: 2;
   t_config_el1_rul1: 4; (минут)
t_config_el1_rul2: 2;
t_config_el2_rul1: 0.5;
t_config_el2_rul2: 1;
t_config_el3_rul1: 9.5;
t_config_el3_rul2: 10;
}
```

В данном примере мы видим, что зафиксировано необходимое потраченное время для выполнения настройки конфигурации средств защиты информации для предоставления доступа в каждом конкретном случае. На разграничение доступа к 1-й

папке (el1) на чтение (rul1) нужно потратить в среднем 4 минуты, на предоставление такого же доступа ко 2-й папке (el2) нужно меньше времени, а именно полминуты, возможно это связано с тем что папка меньше или ее не нужно долго искать. Также мы видим, что время, затраченное на доступ к третьей папке, существенно отличается. Таким образом можно задавать конкретные значения потраченных временных ресурсов на каждую операцию, что, в свою очередь, может помочь использовать более точный метод распределения при моделировании процедуры обработки запроса на предоставление прав доступа.

Заключение.

Таким образом рассмотрены возможные логико-языковые средства для описания систем УПД. Приведен пример на языке JSON, где для каждого действия оператора определено время. Задавая эти параметры в математические модели систем УПД с использованием средств автоматизации возможно проводить нагрузочные испытания. Предлагается использовать математический аппарат систем массового обслуживания для проведения таких испытаний.

## СПИСОК ИСТОЧНИКОВ


1. Андреев О. О. О методах оптимизации механизмов разграничения доступа, основанных на логико-языковых средствах. Проблемы информатики. – 2009. – № 1 (2). – С. 24-33. Доступно по: // http://www.oasis-open.org/.

2. Lorch M. First experiences using XACML for access control in distributed systems / M. Lorch, S. Proctor, R. Lepro et al. // Proc. of the ACM workshop on XML security, 31 Oct., 2003.

3. Fisler K. Policy verification and change impact analysis / K. Fisler, S. Krishnamurthi, L. Meyerovich, M. Carl // Proc. of the workshop Ottawa "New challenges for access control", Ottawa (Canada), 27 Apr. 2005 // Available at: http://sec.cs.kent.ac.uk/permis/.

4. Martin E. Automated test generation for access control policies via change-impact analysis / E. Martin, T. Xie // Proc. of the 3rd Intern. workshop on software engineering for secure systems (SESS 2007), May 2007.

5. Моделирование и верификация политик безопасности управления доступом в операционных система / П. Н. Девянин. – М: Горячая линия – Телеком, 2019. – 214 с.

6. Internet Engineering Task Force (IETF). Request for Comments: 7159. The JavaScript Object Notation (JSON) Data Interchange Format. // https://www.rfc-editor.org/rfc/rfc7159.txt // 26.11.2022 г.


## LOGICAL-LANGUAGE TOOLS FOR DESCRIBING THE ACCESS CONTROL MODEL IN INFORMATION SYSTEMS


***© 2022 A. B. Sizonenko, A. O. Titarev, I. S. Rud***

*Krasnodar Higher Military School (Krasnodar, Russia)*



*The existing logical and linguistic descriptions of access control systems (DACS) are considered, their positive and negative sides are considered. A new method of describing the DACS using the JSON language is proposed for the most accurate analysis of the load on administrators (operators) of information security of information systems, as well as the time required to conduct access control operations in information systems.*



*Keywords: ergatic systems, sociotechnical systems, logical and linguistic means, information security system, users, access rights management, information security tools, powers, queuing system.*