УДК 05.13.01

Проскурняк К.И.,
студентка
Тольяттинский государственный университет,
Россия, Тольятти
e-mail: ksu_saratov@inbox.ru

АСПЕКТЫ РЕАЛИЗАЦИИ МОДЕЛЕЙ РАЗГРАНИЧЕНИЯ ДОСТУПА И НЕДОСТАТКИ СУЩЕСТВУЮЩИХ ПОДХОДОВ В СЕТИ КОРПОРАТИВНЫХ ПОРТАЛОВ

Аннотация: *Представлен обзор дискреционного и мандатного методов разграничения доступа. Выделены достоинства и недостатки рассматриваемых моделей разграничения доступа. Предлагается решение недостатка дискреционного метода разграничения доступа*.

Ключевые слова: доступ, разграничение доступа, метод доступа, дискреционный метод разграничения доступа, мандатный метод разграничения доступа, субъект, объект.

Proskurnyak K.I.,
student
Togliatti State University,
Russia, Togliatti

ASPECTS OF IMPLEMENTATION OF ACCESS CONTROL MODELS AND DISADVANTAGES OF EXISTING APPROACHES IN THE CORPORATE PORTAL NETWORK

Abstract: *An overview of discretionary and mandatory methods of access control is presented. The advantages and disadvantages of the considered access control models are highlighted. A solution to the disadvantage of the discretionary method of access differentiation is proposed.*

Keywords: access, access differentiation, access method, discretionary access differentiation method, mandatory access differentiation method, subject, object.

Введение.

Цель настоящего исследования – определить аспекты реализации моделей разграничения доступа и недостатки подходов в сети корпоративных порталов [1].

Методика исследований.

Методика исследования базируется на основных целях построения любой системы защиты информации – обеспечение конфиденциальности, целостности и доступности защищаемых информационных ресурсов [2]. При этом обеспечение информационной безопасности (ИБ) – это комплексная задача, решаемая параллельно по целому ряду направлений: правовому, организационному и техническому. Для реализации аспектов ИБ можно использовать различные методы разграничения доступа. Метод доступа к объекту – операция, которая определена для данного объекта. Ограничить доступ к объекту возможно именно с помощью ограничения возможных методов доступа.

Результаты исследований.

Существенным недостатком дискреционных моделей является то, что в ходе функционирования структура информационных систем изменяется таким образом, что субъекты и объекты могут меняться местами [3, 4, 5]. Так, информационные системы рассматривались ранее как объект управления, в то время как человек-пользователь являлся субъектом управления.

Но при включении человека в информационную систему его роли разделились на исполнительную и управляющую [6]. Человек-исполнитель теперь является объектом управления, а человек с ролью управления является субъектом управления.

С целью устранения недостатков матричных моделей были разработаны так называемые многоуровневые модели защиты, классическими примерами которых являются модель конечных состояний Белла и Ла-Падулы, а также решетчатая модель Д. Деннинг. Многоуровневые модели предполагают формализацию процедуры назначения прав доступа посредством использования так называемых меток конфиденциальности или мандатов, назначаемых субъектам и объектам доступа [7, 8].

В тоже время, с целью обеспечения единых подходов к обеспечению разграничения доступа, непрерывного мониторинга и контроля состояния системы защиты, сокращения сроков модернизации, модификации и

восстановления существующей системы разграничения доступа в ходе жизнедеятельности организации, значительную роль играет корректное отражение реализованной системы разграничения доступа [9, 10].

Существующие механизмы дискреционного, мандатного, ролевого разграничения доступа позволяют обеспечить реализацию необходимых мер защиты информации, но само корректное и подробное описание применяемых политик настройки средств защиты и программных продуктов [11].

Объем матрицы доступа, в которой будет подробно расписано дискреционный принцип доступа даже для 30-50 пользователей, работающих в сети предприятия [12].

Описание модели мандатного разграничения доступа, как правило, сводится к высшему грифу конфиденциальности и весьма формальному описанию местоположения защищаемых ресурсов [13].

Аналогичная проблема существует и при описании других моделей. Анализ вышеизложенного материала позволяет сделать вывод, что даже применение различных средств автоматизации процесса формирования и описания полномасштабной матрицы доступа принесут определенный положительный эффект, но это только половинчатая мера [14, 15]. Необходимо кардинальное решение данной проблемы.

Обсуждение результатов.

Одним из способов является переход от статической к динамической матрице доступа, формируемой на основе пула разрешенных маршрутов с обязательным автоматическим действий пользователя [16].

Для решения задачи по определению правил разграничения доступа к вновь создаваемым информационным ресурсам предлагается представить информационную систему в виде логически связанных узлов [17].

Узел – это пользователь без привязки роли администратора или роли пользователя. Ввиду большого количества вариантов движения информационного ресурса в процессе его создания, корректировки (отладки), ознакомления, визирования, принятия решения и тому подобное, и сложности их

описания (вариантов), предлагается непосредственное определение перечня допущенных узлов возложить на главенствующий сетевой узел на каждом этапе решения той или иной задачи [18].

Например, исполнитель на своем узле И1 определяет порядок и права доступа к нему последующего узла (начальник Н1).

На данном этапе главенствующим узлом является И1. Начальник Н1 после выполнения своих функций ознакомления, визирования и т.п., определяет следующий узел и его права.

Доступ предыдущего узла И1 при этом может быть аннулирован. Основная идеология данного базируется на том постулате, что должностное лицо (главенствующий узел) в данный момент времени несет основную ответственность за содержание и обеспечение безопасности информационного ресурса [19, 20].

При этом, выбор исполнителем И1 следующего узла, например Н1, осуществляется из набора разрешенных к взаимодействию узлов И1 – И3, Н1 – Н2 и т.д.

Выводы.

Использование данного подхода позволяет вместо описания всевозможных вариантов движения в матрице доступа описать только разрешенный набор взаимодействующих узлов, а процесс модификации, удаления, передачи возлагается на автоматизированную систему действий каждого участника процесса [21].

Список литературы:

1. Ерёменко В.Т., Фисун А.П., Константинов И.С. Актуальные теоретические и технологические аспекты информатики: Методологические основы информатики: Монография Том 1. Орёл: ОГУ, Орел. ГТУ, 2018. 234 с.

2. Андерсон Д.А. Дискретная математика и комбинаторика. М.: Вильяме, 2016. 960 с.

3. Хорошевский В.Г., Курносов М.Г., Мамойленко С.Н., Поляков А.Ю. Архитектура и программное обеспечение пространственно-распределённых вычислительных систем // Вестник ГОУ ВПО «СибГУТИ». 2018. № 2. С. 112-122.

4. Балавин М.А. Развитие систем автоматизации в ОАО «Газпром» // Газовая промышленность. 2016. № 10. С. 22.

5. Вендров А.М. Проектирование программного обеспечения экономических информационных систем. М: «Финансы и статистика», 2015. 544 с.

6. Воеводин В.В. Распределенные системы, принципы и парадигмы // Вторая сибирская школа-семинар по параллельным вычисления. Томск: Изд-во ТГУ, 2016. С. 3-9.

7. Воеводин В.В. Параллельные вычисления. СПб.: БХВ-Петербург, 2015. 608 с.

8. Воеводин В.В. Распределенные вычисления - от теории к практике // Всероссийская научно-методическая конференция Телематика-2003. СПб.: РИО СПбИТМО СПб, 2013. С. 246-247.

9. Вульф Б. Шаблоны интеграции корпоративных приложений. Проектирование, создание и развертывание решений, основанных на обмене сообщениями. М.: ООО «И.Д. Вильяме», 2015. 672 с.

10. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. Екатеринбург: Издательство Уральского университета, 2013. 328 с.

11. Грекул В.И. Проектирование информационных систем. Интернет-университет информационных технологий. М.: «БИНОМ», 2015. 304 с.

12. Грушко А.А. Теоретические основы защиты информации. М.: Яхтсмен, 1996. 192 с.

13. Девянин П.Н. Модели безопасности компьютерных систем: Учебное пособие для студ. высш. учеб. заведений. М.: Издательский центр «Академия», 2015. 144 с.

14. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2016. 176 с.

15. Демидов А.В. Модель подсистемы разграничения доступа системы управления информационным обменом сети корпоративных порталов // Прикладная математика, управление и информатика. 2016. Т. 1. С 65-68.

16. Демидов А.В. Проектирование подсистемы разграничения доступа к порталам органов государственной власти // Информационное развитие России состояние, тенденции и перспективы (региональный аспект). Сборник научных статей 2-й межрегиональной научно-практической конференции . 2017. С. 5-11.

17. Демидов А.В. Обратный прокси-сервер в рамках системы управления информационным обменом сети web-порталов // Информационные системы и технологии (ИСиТ-2014). 2014. Т. 1. С. 170-174.

18. Демидов А.В. Анализ и выбор протоколов взаимодействия распределенных компонентов системы управления информационным обменом сети корпоративных порталов // Информационные системы и технологии (ИСиТ-2014). 2014. Т. 1. С. 180-185.

19. Демидов А.В. Моделирование процессов информационного обмена с приоритетами в сетях передачи данных промышленных предприятий // Информационные технологии в науке, образовании и производстве. 2016. Т. 5. С. 94-101.

20. Еременко В.Т. Функциональная стандартизация протоколов информационного обмена в распределенных управляющих системах: дис. … доктора тех. наук. Орёл, 2015. 404 с.

21. Ерёменко В. Актуальные технико-экономические и организационные аспекты информатизации В 2-х кн.: Кн. 1. Том 3. Орёл : ОГУ, ГУ-УНПК, 2016. 180 с.