DOI: 10.12731/2306-1561-2013-4-33

ACCESS RIGHTS IN COMPUTER NETWORKS

Sumkin K.S.

Abstract

The article describes the research, development model differentiation of access rights users to improve administrative efficiency in computer networks. The methods of fuzzy giperrezolyutsii, orthogonal Latin squares to solve the problem of determining the parameters of access to each specific situation. The methods of fuzzy inference to determine access rights.

Keywords: *access rights, fuzzy logic.*

УДК 004.896

РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА В КОМПЬЮТЕРНЫХ СЕТЯХ

Сумкин К.С.

Аннотация

В статье рассмотрены: исследование, разработка модели разграничения прав доступа пользователей для повышения эффективности администрирования в компьютерных сетях. Предложены методы нечеткой гиперрезолюции, ортогонально–латинских квадратов для решения задачи определения параметров доступа в каждой конкретной ситуации. Предложены методы нечеткого логического вывода для определения прав доступа.

Ключевые слова: *разграничение прав доступа, нечеткая логика.*

Введение

В настоящее время увеличивается использование компьютерных сетей во всех сферах жизни современного общества: в сфере обороны, экономики, транспорта, промышленности, связи, здравоохранения, в государственных организациях, в финансовых и банковских структурах, в области защиты и обеспечения правопорядка. Поэтому остро стоят вопросы информационного контроля и управления правами пользователей в компьютерных сетях. Разграничение прав доступа пользователей один из основных компонентов работы компьютерных сетей.

Актуальной задачей является противодействие несанкционированному доступу (НСД) к ресурсам компьютерных сетей, а именно безопасное управление доступом и информационными потоками по памяти и по времени между сущностями компьютерной системы. В связи с увеличением объемов обмена информацией,

количества поставщиков и пользователей, а также возрастанием плотности информационных потоков и усложнением их структуры, растет нагрузка на компьютерные сети. Из–за нарушения правил доступа, а также действий со стороны лиц, не имеющих прав доступа к ресурсам компьютерных сетей, основной проблемой является разработка эффективных моделей разграничения прав доступа (РПД) пользователей и их программная реализация.

Для достижения поставленной цели решены следующие основные задачи:

- проведен анализ современных моделей, методов, алгоритмов и программных средств РПД пользователей в компьютерных сетях, выявлены основные проблемы и осуществлен выбор путей их решения;
- разработан оригинальный метод для определения информационных ресурсов (доступных пользователю), основанный на применении методов нечеткой гиперрезолюции и ортогонально–латинских квадратов, обеспечивающий учет параметров доступа в каждой конкретной ситуации РПД пользователей компьютерных сетей;
- предложена оригинальная модель РПД для компьютерных сетей с различными уровнями иерархии пользователей и разработан алгоритм реализации данной модели;
- разработаны модель и алгоритм управления информационными потоками (по памяти и по времени) между ресурсами компьютерных сетей.

Обзор существующих подходов РПД пользователей в компьютерных сетях

Рассмотрены отечественные и зарубежные программные и аппаратные средства, с помощью которых осуществляется РПД пользователей в современных операционных системах. В частности, рассмотрены следующие программные средства: продукты фирмы Microsoft (операционные системы Windows Server NT/2000/2003, Windows XP/Vista) , ОС Novell Netware и LINUX (RedHat, Ubuntu). В качестве рассмотренных аппаратных средств выступают системы разграничения доступа «КРИПТОН — Щит», а также Secret Net. Отмечены положительные и отрицательные стороны средств [1].

Исследованы модели РПД пользователей в компьютерных сетях. К ним относятся каноническая модель, а также базовые модели доступа: модель Take – Grant и её основные расширения, модель Белла – ЛаПадула и её интерпретации, модель систем военных сообщений, модель ролевого разграничения доступа [3]. В качестве типового решения, характерного для рассмотренных программных и аппаратных средств РПД пользователей компьютерных сетей, является использование модели ролевого разграничения доступа, функционирование которой проиллюстрировано на рисунке 1 [1].

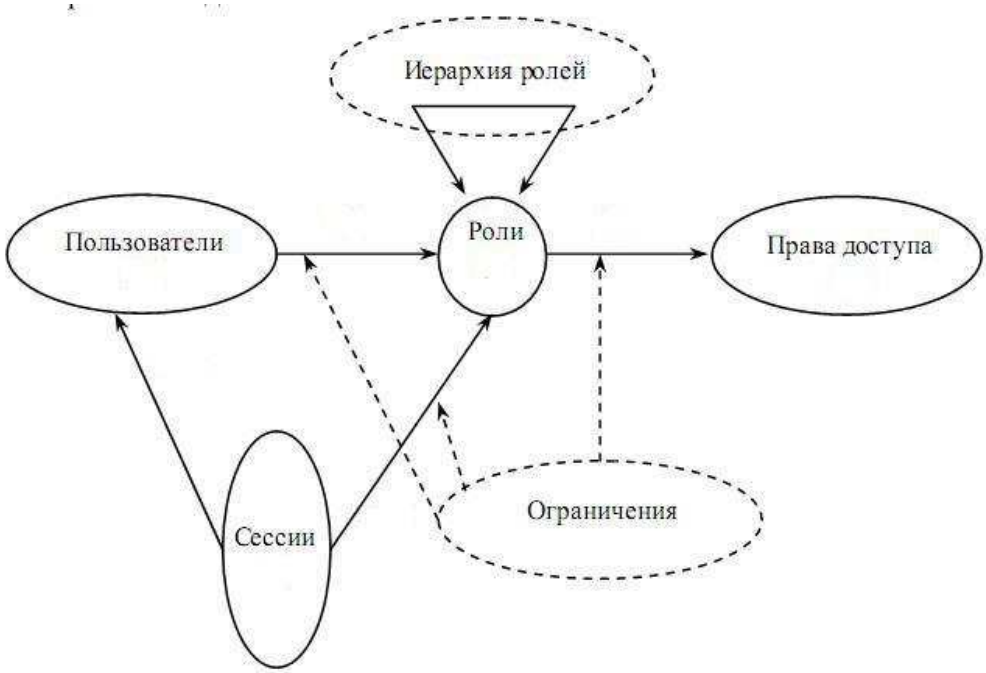

Рисунок 1 - РПД пользователей компьютерных сетях

Значительное внимание при РПД уделено эффективности администрирования в компьютерных сетях, то есть комплексу мер, проводимых при РПД пользователей с целью обеспечения санкционированного доступа к ресурсам сети. Эффективность определяется следующими показателями: отказоустойчивость, возможность получения НСД, скорость работы системы, получение санкционированного доступа.

Показано, что классические модели по РПД пользователей не позволяют учитывать различные уровни иерархии субъектов, коэффициенты важности и доверия, а также параметры доступа пользователей к ресурсам [9 – 12].

Анализ возможных путей решений задачи РПД, способных учесть различные уровни иерархии субъектов, коэффициенты важности и доверия, а также параметры доступа пользователей к ресурсам показал, что для решения подобной задачи могут быть использованы подходы на основе использования нейросетевой технологии, нечеткого логического вывода (Мамдани, Ларсена, Цукамото, Сугэно 0 порядка, Такаги – Сугэно), ортогонально–латинских квадратов.

При выборе подхода к решению поставленных задач основным фактором являлась необходимость обеспечения принятия решения в обстановке неполной и нечеткой информации. Поэтому модель РПД пользователей компьютерных сетей должна быть максимально приближена к рассуждениям человека, учитывать различные уровни иерархии пользователей, а также отслеживать злоупотребления служебными полномочиями и ошибки конфигурации [6]. Соответственно при выборе метода определения параметров доступа пользователей к ресурсам системы в качестве основного фактора было выбрано удобство моделирования РПД [5].

Теоретические вопросы разработки модели РПД пользователей компьютерных сетей

Под объектом понимается любой элемент компьютерных сетей

$$O = \{O_1, O_2, ..., O_k\}.$$

В качестве объекта доступа $O_i \ \ (i = \overline{1,k})$ рассматривается как отдельный объект, так и группа объектов, характеризуемых одинаковыми для них правами доступа [2].

Под субъектом понимается любая сущность, способная инициировать выполнение операций над объектами $S = \{S_1, S_2, ..., S_k\}$ [2].

Под доступом понимается выполняемая операция, определенная для некоторого объекта.

Сформулируем утверждение о возможности доступа субъекта к объекту, в соответствии с которым субъект S_i может получить доступ к объекту O_i, если существует субъект S_{i+1}, имеющий доступ d_{ij}, к элементу O_i такой, что субъекты S_i и S_{i+1} связаны бинарным отношением ρ, содержащим хотя бы одно из возможных прав. Рассмотрены и доказаны все возможные случаи исходных условий доступа.

Для идентификации прав субъекта на определенный объект, а также для автоматизации процесса РПД пользователей введены рабочие определения специальных матриц «доверия» и «важности».

Определение 1. Матрица важности объектов - это квадратная матрица, состоящая из коэффициентов шкалы ценности [0,1], которые определяются субъектами (пользователями) и соответствуют степени важности обрабатываемой информации на объекте.

Определение 2. Матрица доверия субъекту - это вектор, коэффициенты которого определяются экспертом (в соответствии со шкалой [0,1]) и показывающие возможность субъекта изменять или добавлять информацию на объекте.

Представим базовую модель ролевого разграничения доступа, описывающую права работы субъекта с объектом (внесение информации на объект, права обработки субъектом информации, изменения информации). Как развитие данной модели за счет введенных матриц доверия и важности была предложена и исследована модель РПД вида $R = AC$, где R - вектор, состоящий из кандидатов субъектов на получение права доступа, A - матрица важности, имеющая размерность $n \times n$, C - вектор-столбец доверия размерностью n. Выбор максимума из элементов вектора R, происходит путем перебора всех его элементов, что позволяет определить право субъекта на объект.

Существенным отличием данной модели является возможность учета коэффициентов важности и доверия при определении прав субъекта на объект.

С помощью предложенной модели права субъекта на объект определяются только в тех случаях, когда субъекты имеют возможность однозначно определять права на объект. Однако, эта модель не учитывает такие характеристики РПД как степень

важности обрабатываемой информации, степень необходимости в конкретной информации для того или иного субъекта, степень возможной опасности, исходящей от каждого субъекта и др.

С этой целью на основе дальнейших исследований были выявлены и унифицированы параметры, при которых субъект, как правило, получает доступ к объекту.

Определение 3. Параметры доступа (ПД) - это переменные, с помощью которых определяется доступ субъектов $S_1, S_2, ..., S_n$ к объектам $O_1, O_2, ..., O_m$.

В таблице 1 представлен пример возможных значений ПД (где sec — степень важности обрабатываемой информации, nei - степень необходимости в конкретной информации для субъекта, dng — степень возможной опасности исходящей от каждого субъекта).

Таблица 1 – Пример значений ПД

Переменная / **Параметр**	**1**	**2**	**3**
sec	Не важная	Важная	Очень важная
nei	Не нужная	Нужная	Жизненно необходимая
dng	Минимальная	Средняя	Максимальная

Субъект получает доступ к объекту при наличии соответствующих значений ПД. С этой целью введено определение существенных параметров доступа.

Определение 4. Существенные параметры доступа - это значения ПД, которые необходимы для получения доступа субъектов к объектам.

Для определения информационных ресурсов (доступных пользователю) необходимо установление существенных ПД для субъекта, в связи, с чем разработан соответствующий метод на основе использования аппарата нечеткой гиперрезолюции и ортогонально–латинских квадратов.

Естественным ограничением для применения метода нечеткой гиперрезолюции с целью определения существенных ПД является ограничение множества значений ПД. В качестве основного ограничения выступило следующее: в том случае, если субъект может пользоваться очень важной информацией, то он также может пользоваться и информацией с более низкой степенью важности.

Приведем описание представления ПД в виде лингвистических переменных. В качестве множеств значений лингвистических переменных выступают значения, пример которых приведен в таблице 1.

На основе использования аппарата нечеткой гиперрезолюции был разработаем следующий метод.

1. В качестве исходного условия принимается условие, показывающее при каких значениях лингвистических переменных достигается возможность доступа субъекта к объекту:

$$\sec(S_i) \cup nei(S_i) \cup \neg dng(S_i) \cup ur\_d(S_i), \quad (1)$$

где (S_i) — субъект, а ur_d — количественный показатель для оценки возможности доступа субъекта к объекту.

2. В случае, если в семантической процедуре лингвистической переменной не описано преобразование, то эксперт определяет $\sec(S_i), nei(S_i), \neg dng(S_i)$ для данного субъекта.

3. Определяется значения ur_d для субъекта (S_i), которое сравнивается с некоторой нижней границей и делается вывод о соответствии существенных ПД для субъекта (S_i).

Данный метод определения существенных ПД не позволяет в полной мере автоматизировать процесс РПД пользователей в компьютерных сетях из–за необходимости постоянного привлечения эксперта для определения $\sec(S_i), nei(S_i), \neg dng(S_i)$. С целью повышения степени автоматизации процессов взаимодействия с экспертом (соответственно снижение нагрузки на администраторов) введено понятие о функциональных матричных блоках, удобных для моделирования РПД по существенным ПД.

Суть предложенного подхода заключается в следующем пусть X_i' — множество векторов переменной длины от 1 до (n_i), где $i = \{\overline{1, N}\}$, N – количество значений ПД, $L(W_i, w_i, X_i')$ — «латинское преобразование» и $X_i' \approx Z_j$.

Тогда, приняв $Z_j = NX_i$, выражение для «одноканальной» инверсии многозначной логики будет иметь вид:

$$NX_i = L(W_i, w_i, X_i'). \quad (2)$$

При умножении базовой матрицы и построенных ортогонально – латинских квадратов вычисляются значения результирующей матрицы. Элементы результирующей матрицы соответствуют рекомендациям о том, какими существенными ПД обладает субъект. Детальное описание алгоритма, реализующего данный метод, и результаты эксперимента приведены в разделе 3.

Предложенный подход определения существенных ПД позволил построить модель РПД субъектов к объектам. Пусть субъекты и объекты представляются в виде следующих нечетких множеств:

$$O' = \{\mu_O(x) / x\}, \quad (3)$$

где x — элемент множества объектов, а $\mu_O(x)$ — характеристическая функция принадлежности;

$$S' = \{\mu_S(y)/y\}, \quad (4)$$

где y — элемент множества субъектов, а $\mu_S(y)$ — характеристическая функция принадлежности, причем функции принадлежности $\mu_O(x)$ и $\mu_S(y)$ принимают собственные значения в некотором упорядоченном множестве [0,1]. Каждый элемент множеств субъектов и объектов рассматривается как собственное нечеткое подмножество. В этом случае можно рассматривать не отдельные элементы субъектов и объектов, а принадлежность элементов нечетким подмножествам.

Предложим формализм представления нечетких продукционных правил и алгоритм нечеткого логического вывода (НЛВ). Главное отличие разработанного алгоритма от традиционных методов НЛВ (в частности, Мамдани, Цукамото, Сугэно 0 порядка и других) заключается в том, что в правилах используется не только нечеткая импликация Мамдами, но и любые вычисления, необходимые для получения доступа.

Нечеткие продукционные правила, строятся следующим образом [4]:

$$\Pi_i: \text{ЕСЛИ } y \text{ есть } \mu_S(y)_i \text{ И } x \text{ есть } \mu_O(x)_i \text{ И(ИЛИ) sec есть } L \text{ И(ИЛИ) } nei \text{ есть } M \text{ И(ИЛИ) } dng \text{ есть } N \text{ ТО } d_i = \rho^{-1}, \quad (5)$$

где Π_i — правило доступа субъекта к объекту $i = \overline{\{1,n\}}$, где n — количество правил.

Опишем этапы разработанного алгоритма НЛВ [7].

Этап 1. Фазификация.

Этап 2. Вычисление степеней срабатывания предпосылок по каждому из правил — α_i (по методу, выбранному экспертом).

Этап 3. Активизация заключений по каждому из правил — $< \alpha_i, \beta_i | \beta_i = f_i\ (\alpha_i) >$, где $f_i\ (\alpha_i)$ — функция доступа субъекта к объекту с параметром α_i, вычисляемым на втором этапе.

Этап 4. Дефазификация.

$$D = \frac{\sum_{i=1}^{n} \alpha_i d_i}{\sum_{i=1}^{n} \alpha_i}, \quad (6)$$

где D — значение доступа i — го субъекта к i — му объекту.

В предложенном алгоритме вместо непрерывной функции используется дискретная функция, так как разграничение прав – процесс дискретный.

Если построить обратную функцию доступа нельзя или её определение в ряде случаев невозможно, то тогда применяется алгоритм нечеткого логического вывода Сугэно 0 порядка. В этом случае значение доступа присваивается в виде константы. Тогда база нечетких продукционных правил формируется следующим образом [8, 9, 11, 12]:

$П_i$: ЕСЛИ y есть $\mu_S(y)_i$ И x есть $\mu_O(x)_i$ И(ИЛИ) sec есть L И(ИЛИ) nei есть M И(ИЛИ) dng есть N ТО $d_i = const_i$. (7)

Этапы разработанного алгоритма НЛВ аналогичны предыдущему, за исключением второго этапа, который имеет следующий вид.

Этап 2. Вычисление степеней срабатывания предпосылок по каждому из правил $const_i$.

Таким образом, построена модель РПД в компьютерных сетях, основанная на формализме нечетких продукционных правил (5), (7), которые описывают доступ субъектов к объектам, что обеспечивает учет параметров доступа, а также различные уровни иерархии пользователей.

Кроме того, разработаем модель создания информационных потоков по памяти и по времени. С этой целью введено значение порогового значения $(Dpor)$, при котором доступ для субъекта разрешен и создается информационный поток по времени. Если значение доступа D, определяемое по формуле (6), больше или равно пороговому значению $Dpor$, при котором доступ к объекту разрешен, то создается информационный поток по времени. В этом случае, модель создания информационных потоков по времени представляется в виде [8]:

$$can\_(права)\_time = \begin{cases} 1, если \ \mathrm{D} \geq Dpor \\ 0, если \ \mathrm{D} < Dpor \end{cases}. \quad (8)$$

Таким образом, получено решение актуальной задачи разграничения прав доступа пользователей к ресурсам компьютерных сетей, которое позволяет учитывать существенные ПД.

Алгоритмизация разработанных моделей и методов, а также проектирование программного обеспечения РПД

На основе описанных во втором разделе методов нечеткой гиперрезолюции и ортогонально – латинских квадратов разработаем пошаговый алгоритм реализации модели РПД субъектов к объектам.

Шаг 1. Определение существенных ПД по формулам (1), (2).

Шаг 2. Если новых значений ПД не было, или их количество не превышает 18, тогда применение метода многозначной логики, иначе использование смешанного метода многозначной логики и гиперрезолюционного вывода.

Шаг 3. Замена всех множеств субъектов и объектов соответствующими нечеткими множествами по формулам (3), (4).

Шаг 4. Построение функции принадлежности для объекта и субъекта.

Шаг 5. Формирование базы нечетких продукционных правил по формулам (5) или (5), (7).

Шаг 6. Выбор механизма НЛВ. Определение этапов нечеткого логического вывода для каждого алгоритма по формуле (6).

Шаг 7. Если значение, вычисленное по формуле (6), не превышает порогового значения, то создание информационного потока по времени по формуле (8).

В результате выполнения этапа дефаззификации данного алгоритма получается значение доступа D, на основе которого происходит создание информационного потока по времени. Создавать информационный поток по памяти нецелесообразно, что облегчает работу информационной системы и не нагружает память лишними данными.

На основе разработанных алгоритмов построена архитектура программной системы. В архитектуру программной системы входит четыре подсистемы: подсистема определения пользователей (характерной особенностью системы является идентификация и аутентификация, обеспечивающие процесс взаимодействия с подсистемой определения доступа); подсистема определения ПД (в которую входит средство определения существенных ПД); подсистема определения доступа (в которую входит нечеткий решатель, а также средство создания информационных потоков); подсистема ведения журналов событий.

Заключение

Таким образом, проведен анализ современных моделей, методов, алгоритмов и программных средств РПД пользователей в компьютерных сетях, выявлены основные проблемы и осуществлен выбор путей их решения;

Разработан оригинальный метод для определения информационных ресурсов (доступных пользователю), основанный на применении методов нечеткой гиперрезолюции и ортогонально–латинских квадратов, обеспечивающий учет параметров доступа в каждой конкретной ситуации РПД пользователей компьютерных сетей.

Предложена оригинальная модель РПД для компьютерных сетей с различными уровнями иерархии пользователей и разработан алгоритм реализации данной модели;

Разработаны модель и алгоритм управления информационными потоками (по памяти и по времени) между ресурсами компьютерных сетей.

Список информационных источников

[1] Сумкин К.С., Морозова Т.Ю., Никонов В.В. Методы управления доступом к информационным ресурсам автоматизированных систем управления на основе канонической модели.// Приборы и системы. Управление. Контроль. Диагностика, 2008, № 10, с. 21 – 23.

[2] Сумкин К.С., Морозова Т.Ю. Об использовании нечетких множеств для разграничения прав доступа информационной сети. // Наукоемкие технологии, 2008, №7, т.9, с. 12–14.

[3] Сумкин К.С., Морозова Т.Ю. Использование канонической модели для разграничения прав пользователей локальной вычислительной сети. Сборник трудов X научной Всероссийской научной – технической конференции “Новые информационные технологии». – М.: МГУПИ, 2007, с. 113– 118.

[4] Сумкин К.С., Морозова Т.Ю. Модели контроля доступа к ресурсам системы. Сборник трудов Международной научно – практической конференции

«Современные направления теоретических и прикладных исследований». – Одесса: Черноморье, 2007, с. 11 – 15.

[5] Сумкин К.С., Морозова Т.Ю. Использование нечетких множеств для управления доступом пользователей к ресурсам системы в условиях неопределенности. Сборник трудов Международной научно – практической конференции «Современные направления теоретических и прикладных исследований». Том 5 – Одесса: Черноморье, 2008. С. 48– 52.

[6] Сумкин К.С. Об использовании теней нечетких множеств для разграничения прав доступа пользователей. Сборник научных трудов по материалам международной научно - практической конференции «Перспективные инновации в науке, образовании, производстве и транспорте». Одесса, 2008, с. 31–35.

[7] Сумкин К.С., Никонов В.В. О некоторых методах защиты средств вычислительной техники. Новые информационные технологии: Сборник трудов 10 Всероссийской научно - технической конференции (Москва, 19 - 20 апреля 2007 г.) / Под ред. А.П. Хныкина, А.Ю. Выжигина. – М.: МГУПИ, 2007, с. 45–51.

[8] Сумкин К.С. Методы нечеткой логики для обеспечения безопасной работы пользователей сети. Современные технологии в задачах управления, автоматики и обработки информации // Труды 17 международного научно – технического семинара. Алушта, сентябрь 2008 г, с. 60 – 61.

[9] Остроух А.В. Исследование начального периода моделирования на точность среднеинтегральной оценки имитационных моделей / А.В. Остроух, А.А. Солнцев, Н.В. Солдатов, К.А. Новицкий, П.С. Якунин // Вестник МАДИ. – 2010. - Вып. 2(21). - С. 61-65.

[10] Антонов П.Д. User Is A Great Obstacle For Security Systems / П.Д. Антонов, А.В. Остроух // Молодой ученый. - 2011. - №4. Т.3. - С. 62-63.

[11] Остроух А.В. Основы построения систем искусственного интеллекта для промышленных и строительных предприятий: монография / А.В. Остроух. – М.: ООО «Техполиграфцентр», 2008. - 280 с. - ISBN 978-5-94385-033-2.

[12] Остроух А.В. Системы искусственного интеллекта в промышленности, робототехнике и транспортном комплексе: монография / А.В. Остроух - Красноярск: Научно-инновационный центр, 2013. – 326 с. - ISBN 978-5-906314-10-9.