УДК 004.45
doi:10.15217/issn1684-8853.2016.1.110

ВОПРОСЫ ТЕРМИНОЛОГИИ. КАК ПРАВИЛЬНО: ПРАВА И/ИЛИ РАЗРЕШЕНИЯ?

А. В. Гордеев[a], *доктор техн. наук, профессор*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Введение: *в абсолютном большинстве публикаций, в том числе в учебной литературе, термины «права» и «разрешения», которые используются при описании методов управления доступом и конкретных правил доступа к информационным ресурсам в информационных системах, отождествляются, т. е. авторы не видят между ними различий, что приводит к тому, что достаточно часто существенно изменяется и искажается смысл.* ***Цель:*** *анализ понятий «права» и «разрешения» с определением областей их корректного применения.* ***Результаты:*** *анализ происхождения этих терминов, их истинного значения и механизмов реализации в информационных системах показал, что термин «права» непосредственно связан с понятием авторизации, и его следует использовать для обозначения полномочий пользователя, а термин «разрешения» — для описания тех действий, которые можно или нельзя применять по отношению к конкретным экземплярам информационных объектов.* ***Практическая значимость:*** *корректное использование терминов «права» и «разрешения» не только повысит культурный уровень специалистов в области информационных систем, но и приведет к более полному взаимопониманию при общении и точности изложения особенностей информационных систем.*

Ключевые слова *— права, разрешения, терминология, управление доступом.*

Введение

В литературе по POSIX-системам [1–3] при описании условий доступа тому или иному пользователю или процессу к некоторому файлу достаточно часто встречается словосочетание «File Rights» — права на файл. Англоязычный термин «Rights» переводится на русский язык как «права». В то же самое время при работе с современными операционными системами компании Microsoft, которые в настоящем в основном используют файловую систему NTFS, и при чтении соответствующей документации на английском языке мы сталкиваемся с использованием термина «Permissions» — «разрешения». В большинстве версий этих операционных систем, локализованных для Российской Федерации (например, в распространенных Windows 8.1 и в серверной версии Windows Server 2008), на вкладке Безопасность (Security) свойств файла можно увидеть слова «разрешения» [4–7]. Однако в технической литературе наши авторы очень часто употребляют термин «права на файлы» при описании не только POSIX-систем, но и Windows-систем. Эти же термины употребляют и при описании условий доступа к другим информационным ресурсам. Поэтому следует, разобрав эти термины, понять, что и когда лучше использовать.

Права на файлы в POSIX-системах

Как известно, к POSIX-системам относятся все те операционные системы, которые удовлетворяют спецификациям POSIX [1]. Они описаны в серии стандартов, разработанных Комитетом 1003 при американском Институте инженеров по электротехнике и электронике (IEEE), и своей целью, прежде всего, имели унификацию и стандартизацию UNIX-систем. Широко известные и все более популярные системы GNU/Linux являются POSIX-системами. К POSIX-системам относятся различные BSD-системы, семейство MAC OS, семейство систем реального времени QNX и многие другие. Во всех этих системах при описании доступа к файлам принято использовать термин «права на файлы». И речь там идет о праве на чтение некоторого файла, праве на его исполнение и праве на запись в этот файл. Эти права определяются для владельца файла, для группы этого владельца и для всех остальных пользователей. Это классика, и ее знают все, кто изучал POSIX-системы.

Разрешения на доступ к файлам в Windows-системах

После завершения эпохи операционных систем Windows 9x, которые использовали файловые системы FAT32, мы в большинстве случаев сталкиваемся с тем, что нужные нам файлы располагаются на томах с NTFS. Эта файловая система появилась в 1993 г. и изначально была ориентирована на использование в корпоративном секторе, поэтому она получила развитые механизмы разграничения доступа. Система NTFS имеет несколько версий, в настоящее время мы преимущественно сталкиваемся с NTFS v.5.x. Для тех, кто изучил реальные возможности этой файло-

вой системы и часто ее использует, должны быть очевидны такие понятия, как «атомарные разрешения», «стандартные разрешения», «специальные (или особые) разрешения» [6], хотя в современных интерфейсах работы со свойствами безопасности теперь таких словосочетаний уже не встретишь. Термин «разрешения» в компании Microsoft используют как по отношению к локальным файлам и каталогам, так и по отношению к сетевому доступу к папкам с файлами, хотя это совершенно разные разрешения.

Этот же термин — «разрешения» — используют при описании дискреционного метода управления доступом. Напомним, что это метод, при котором информационные ресурсы имеют списки управления доступом (Access Control List — ACL), хотя в теории вместо списков могут применяться матрицы. Каждый элемент списка указывает на разрешение или запрет для некоторого принципала безопасности на конкретные операции, которые потенциально можно выполнить над информационным ресурсом. Сами принципалы безопасности указываются специальными идентификаторами. Количество разрешений и их конкретный состав зависят от класса объекта (класса информационного ресурса).

Однако термин «разрешения» почти не используется ни в обиходе специалистов по информационным технологиям, ни в нашей русскоязычной специальной литературе. Даже когда речь идет о системах и продуктах компании Microsoft [7]. Вместо этого почему-то практически повсеместно используют термин «права». И даже в диссертациях авторы часто используют термин «права», в то время как по смыслу речь идет о «разрешениях». Возможно, что это происходит либо из-за неправильного (некорректного) перевода англоязычной технической литературы, либо «по инерции», поскольку UNIX-системы появились намного (на 20 лет!) раньше, и уже сложились некоторые терминологические традиции.

Понятие «права» в Windows-системах и различия между правами и разрешениями

Что касается термина «права», то в контексте систем компании Microsoft в англоязычной литературе синонимом для слова «Rights» может выступить термин «Privileges» — привилегии, льготы. О правах здесь говорят по отношению к пользователям (или их процессам). Эти права (или привилегии) определяются для локальных встроенных групп. Например, во всех современных системах Windows есть такие группы, как *Администраторы*, *Опытные пользователи*, *Операторы настройки сети*, *Пользователи*, *Пользователи удаленного рабочего стола*, *Операторы архива*, *Репликаторы*, *Читатели журнала событий*, *Гости* и некоторые другие. Любой пользователь может входить в несколько групп, и его права при этом суммируются. Максимально возможными правами обладают члены группы *Администраторы*, а минимально возможными правами обладают *Гости*. Если пользователя не включить ни в одну из вышеупомянутых встроенных локальных групп, то его права не определены, и в первых операционных системах класса NT от компании Microsoft такой пользователь даже не мог войти в систему. Для исправления этого казуса правом работы в современных системах стали обладать члены специальной группы *Прошедшие проверку* (Authenticated Users). А для тех случаев, когда в систему можно зайти без аутентификации (т. е. без ввода пароля), что предпочитает делать большинство пользователей, правом работать на компьютере стали все интерактивные пользователи.

Итак, если учетную запись некоторого пользователя поместить в ту или иную встроенную локальную группу, то он начинает обладать соответствующими *правами*. Заметим, что эти права вступают в силу для пользователя после перерегистрации его в системе, а не с момента включения в группу. Дело в том, что после прохождения аутентификации (процедуры проверки подлинности) пользователь и все его вычислительные процессы получают так называемый маркер доступа. Этот маркер включает в себя идентификатор учетной записи пользователя и идентификаторы всех тех групп, в которые входит его учетная запись. Все обращения (запросы) к операционной системе на выполнение тех или иных операций или сервисов всегда сопровождаются маркером доступа.

Чтобы понять механизм действия прав и разрешений и осознать различия между ними, рассмотрим чуть более подробно работу подсистемы безопасности с вышеупомянутыми ACL. Подсистема безопасности NT берет поочередно ACE-элементы из списка и проверяет их на совпадение с одним из принципалов безопасности, которые составляют маркер доступа. При совпадении сигнатур подсистема безопасности проверяет возможность выполнения запрошенной операции, анализируя ситуацию: на данное разрешение стоит запрет, разрешение, или это действие/разрешение в текущем ACE вообще не определено. Если в ACE на данную операцию для совпадающего принципала из маркера доступа встречается запрет, то далее не проводится никаких проверок и в запрашиваемой операции отказывается. Если запрета нет, то осуществляется дальнейший перебор элементов из маркера доступа, а затем берется следующий элемент.

В конечном итоге, мы либо получаем явный запрет на выполнение операции, либо получаем явное разрешение, либо не получаем разрешение, но при отсутствии явного запрета. Последнее означает, что можно не разрешать то или иное действие без явного запрета. Именно на этом механизме и реализуются как разрешения, так и права пользователей. С той только разницей, что, определяя разрешения на доступ к объекту, можно в явном виде запрещать выполнение той или иной операции для конкретного пользователя, в то время как при определении прав никогда не пользуются запретом, благодаря чему можно обеспечить суммирование прав пользователей.

Теперь собственно о различии разрешений и прав. Если список управления доступом принадлежит обычным файлам, а не системным утилитам или каким-либо иным средствам управления системой, то следует говорить о разрешениях. Если же список управления доступом относится к системной программе (например, оснастке управления дисками или апплету настройки сетевого интерфейса), то речь идет о правах. Другими словами, права определяются для класса объектов, а разрешения — для отдельных экземпляров или подмножеств экземпляров этого класса.

Важно отметить, что права имеют приоритет перед разрешениями. Например, есть право владения объектом (информационным ресурсом). Если пользователь является владельцем ресурса, то он может изменять ACL этого объекта, даже если в ACL для этого пользователя стоят явные запреты на редактирование списка.

Определение (назначение) прав для встроенных локальных групп осуществляется за счет указания в ACL для той или иной системной программы (утилиты) соответствующего ACE. При этом указание идентификаторов безопасности возможно именно для встроенных групп, так как эти идентификаторы известны заранее. Так, во всех ACL для системных программ указан идентификатор безопасности группы *Администраторы*. Именно поэтому они могут делать в системе все. На некоторые системные программы помимо группы *Администраторы* могут быть указаны и некоторые другие группы. Редактирование подобных ACL приводит к переопределению прав пользователей либо к явному определению прав для вновь созданных групп безопасности.

Заключение

Итак, при рассмотрении вопросов доступа к информационным ресурсам в POSIX-системах можно и нужно использовать термин «права» на доступ, хотя не будет ошибкой сказать «разрешения» на доступ. Но если мы имеем дело не с UNIX-подобными системами, то при рассмотрении вопросов доступа к тем или иным ресурсам (например, к тем же файлам) следует употреблять термин «разрешения». Именно так в основном и поступают IT-специалисты, которые говорят на английском языке (они используют термин Permissions, а не Rights).

Литература

1. **Робачевский А. М.** Операционная система UNIX. — СПб.: БХВ-Петербург, 2002. — 528 с.
2. **Немет Э., Снайдер Г., Сибасс С., Хейн Т.** UNIX: руководство системного администратора. Для профессионалов: пер. с англ. — СПб.: Питер, Издательская группа BHV, 2002. — 928 с.
3. **Федорчук А. В.** Доступный UNIX: Linux, FreeBSD, DragonFlyBSD, NetBSD, OpenBSD. — СПб.: БХВ-Петербург, 2006. — 672 с.
4. **Холме Д.** Эффективное администрирование. Ресурсы Windows Server 2008, Windows Vista, Windows XP, Windows Server 2003: пер. с англ. — М.: Русская редакция; СПб.: БХВ-Петербург, 2009. — 768 с.
5. **Моримото Р., Ноэл М., Драуби О., Мистри М.** и др. Microsoft Windows Server 2008 R2. Полное руководство: пер. с англ. — М.: Вильямс, 2012. — 1456 с.
6. **Кастер Х.** Основы Windows NT и NTFS: пер. с англ. — М.: Изд. отдел «Русская редакция «ТОО Channel Trading Ltd», 1996. — 440 с.
7. Управление правами на доступ к данным в Microsoft Office 2010. https://support.office.com/ru-ru/article/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0%D0%BC%D0%B8-%D0%BD%D0%B0-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF-%D0%BA-%D0%B4%D0%B0%D0%BD%D0%BD%D0%BD%D1%8B%D0%BC-%D0%B2-Microsoft-Office-2010-c7a70797-6b1e-493f-acf7-92a39b85e30c?ui=ru-RU&rs=ru-RU&ad=RU (дата обращения: 20.05.2015).

UDC 004.45
doi:10.15217/issn1684-8853.2016.1.110

Terminology Issues: What Should We Say, Rights and/or Permissions?

A. V. Gordeyev[a], Dr. Sc., Tech., Professor, avg@aanet.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: In most literature, including textbooks, the terms “rights” and “permissions” are usually identified. Both these terms are used for describing access control methods and specific rules about the access to data resources in informational systems. Authors often do not see any difference between “rights” and “permissions”. As a result, the meaning can be seriously distorted. **Purpose:** In this paper, we analize the ideas behind "rights" and "permissions", defining the areas of correct usage of these terms. **Results:** The analysis of etymology of these terms, their true meaning and the ways of their realization in information systems showed that the term "rights" is directly associated with the idea of autorization and should be used to designate the user's authority, while "permissions" should be used to describe the actions which can or cannot be performed over specific information objects. **Practical relevance:** The correct usage of the terms “rights” and “permissions” will increase the cultural level of information system specialists. Moreover, it will lead to clearer mutual understanding during the communication on informational system issues.

Keywords — Rights, Permissions, Terminology, Access Control.

References

1. Robachevsky A. M. *Operatsionnaia sistema UNIX* [Operating System UNIX]. Saint-Petersburg, BKhV-Peterburg Publ., 2002. 528 p. (In Russian).
2. Nemeth E., Snyder G., Hein T. R. *UNIX and Linux System Administration Handbook*. 4th Edition. Prentice Hall, 2010. 1344 p.
3. Fedorchuk A. V. *Dostupnyi UNIX: Linux, FreeBSD, DragonFlyBSD, NetBSD, OpenBSD* [Available UNIX: Linux, FreeBSD, DragonFlyBSD, NetBSD, OpenBSD]. Saint-Petersburg, BKhV-Peterburg Publ., 2006. 672 p. (In Russian).
4. Holme Dan. *Windows Administration Resource Kit: Productivity Solutions for IT Professionals Published by Microsoft Press*. Redmond, Washington. 700 p.
5. Morimoto Rand, Noel Michael, Droubi Omar, Mistry Ross. *Microsoft Windows Server 2008 R2 Unleashed*. Sams., 2010. 1680 p.
6. Custer Helen. *Inside the Windows NT File System*. Redmond, Microsoft Press, 1994. 91 p.
7. *Upravlenie pravami na dostup k dannym v Microsoft Office 2010* [Data Access Control in Microsoft Office 2010]. Available at: https://support.office.com/ru-ru/article/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0%D0%BC%D0%B8-%D0%BD%D0%B0-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF-%D0%BA-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%BC-%D0%B2-Microsoft-Office-2010-c7a70797-6b1e-493f-acf7-92a39b85e30c?ui=ru-RU&rs=ru-RU&ad=RU (accessed 20 May 2015).

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.