УДК 004.9
DOI: 10.20310/1810-0198-2016-21-1-146-149

СИСТЕМА ЗАЩИТЫ ДАННЫХ ТЕРМИНУС

© О.В. Крючин, М.А. Рыбаков

Описана система защиты данных Терминус, предназначенная для предотвращения несанкционированного доступа, включая мандатное и дискретное разграничение.
Ключевые слова: мандатный доступ; дискретный доступ; защита данных.

В настоящее время весьма актуальной является проблема защиты данных от несанкционированного доступа. Для ее решения разработано множество инструментов (*SeLinux*, Соболь, *Astra* и т. п.), но все они обладают различными недостатками. Для их преодоления в рамках данной работы создана система Терминус. Недостаток имеющихся реализаций заключается в привязке к конкретной платформе. Система Терминус, напротив, является навесной и, соответственно, может быть установлена на любую поддерживаемую операционную систему семейства *GNU/Linux* (в настоящее время поддерживаются 3 ветки – *Suse, Mandriva* и *Debian*).

Система управления доступом реализована по клиент-серверной схеме. Клиентская часть реализована в виде двух видах – административной и пользовательской. Административная предназначена для управления доступом и защищена паролем (рис. 1). Пользовательская часть предназначена исключительно для управления собственными ресурсами – например, монтирование и отмонтирование флеш-модулей.

Как известно, мандатное управление (принудительный контроль) доступом – это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным системным устройствам и предназначенный для предотвращения их нежелательного использования. Согласно требованиям ФСТЭК (Федеральная служба по техническому и экспортному контролю) мандатное управление доступом или «метки доступа» являются ключевым отличием систем защиты Государственной тайны РФ старших классов 1В и 1Б от младших классов защитных систем на классическом разделении прав по матрице доступа [1].

Рис. 1. Окно авторизации в пенале администрирования системы Терминус

Достоинство данного подхода заключается в том, что пользователь не может полностью управлять доступом к ресурсам (например, документам), которые он создает, поскольку политика безопасности системы, установленная администратором, полностью определяет права (обычно пользователю не разрешается устанавливать более свободный доступ к его ресурсам, чем тот, который установлен администратором) (рис. 2). Тем самым обеспечивается изоляция пользователей и процессов, как известных, так и неизвестных системе.

Описываемая в данной работе система *Terminus* реализует мандатное управление доступом при помощи технологии *ACL* (*Access Control List*). Данная технология расширяет возможности файловой системы *Ext* по управлению доступом. По умолчанию *Terminus* создает несколько уровней доступа – совершенно секретно, секретно, конфиденциально и несекретно. Система настраивает права таким образом, что доступ вверх запрещен всегда, а доступ вниз настраивается для каждой категории. Например, пользователь, входящий в группу «секретно», не имеет доступа к документам, помеченным как «совершенно секретно», а доступ к документам, помеченным как «конфиденциально», настраивается из панели управления системой (рис. 3–4).

В целом, идеи, реализованные в ней, не являются новыми. Изначально такой принцип был воплощен в операционных системах *Flask* и других ориентированных на безопасность операционных системах.

Исследовательский проект *АНБ SELinux* добавил архитектуру мандатного контроля доступа к ядру *Linux*. В *SUSE Linux* и *Ubuntu* есть архитектура мандатного контроля доступа под названием *AppArmor*. Мандатная система разграничения доступа также реализована в ОС *FreeBSD Unix*.

В сертифицированной в системах сертификации Минобороны России и ФСТЭК России операционной системе специального назначения *Astra Linux Special Edition* механизм мандатного разграничения доступа реализован, как и механизм дискреционного разграничения доступа в ядре ОС и СУБД (рис. 3). Решение о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение/запись/исполнение), мандатного контекста безопасности, связанного с каждым субъектом, и мандатной метки, связанной с объектом.

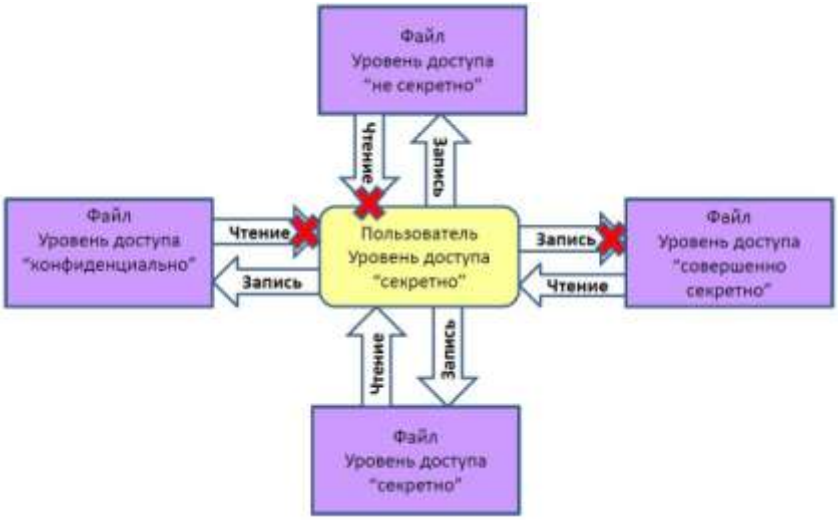

Рис. 2. Схема прав доступа к файлам

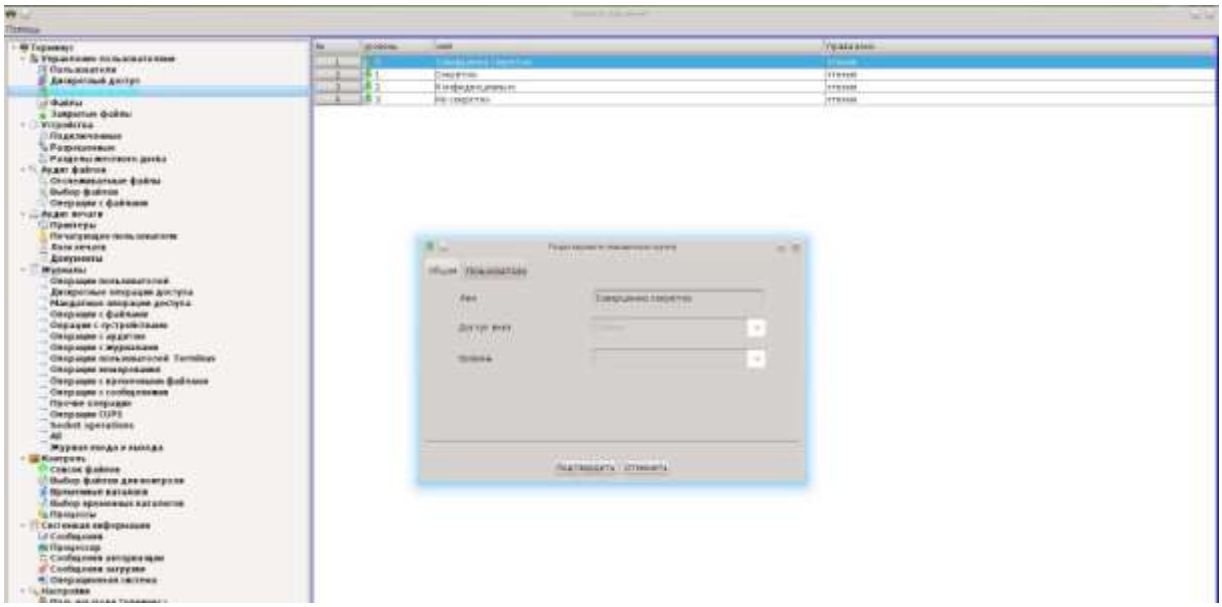

Рис. 3. Редактирование мандатного доступа в системе Терминус

Избирательное (дискретное) управление доступом субъектов к объектам осуществляется на основе списков или матрицы доступа. Для каждой пары (субъект-объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), т. е. тех типов, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту) [2].

Пример настройки матрицы доступа при организации дискреционной модели управления к объектам файловой системы, используемой в дополнение к мандатному механизму.

Возможны различные подходы к построению дискреционного управления доступом. В описываемой в данной работе системе Терминус реализуется следующий подход: каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту [3].

Избирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

Управление доступа к ресурсам включает в себя контроль над съемными устройствами, такими как флеш-модули. По умолчанию автоматическое монтирование съемных устройств отключено. Для его подключения администратор системы должен разрешить это устройство (рис. 4).

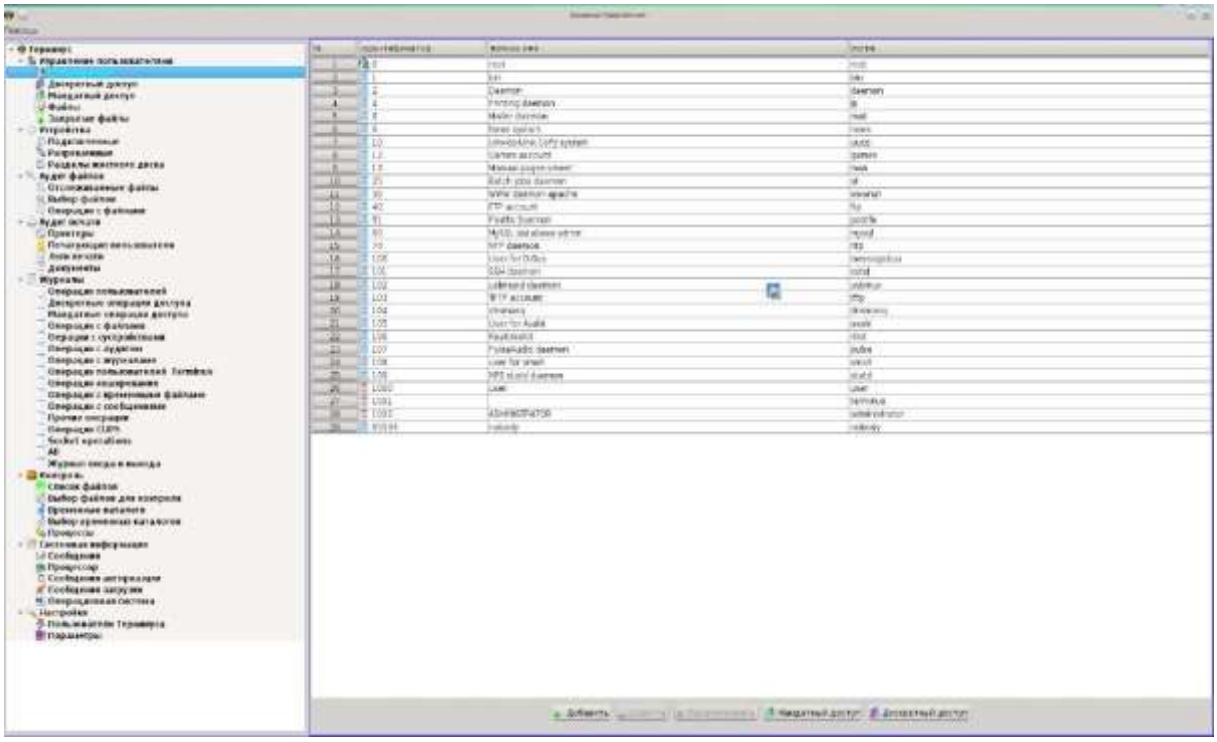

Рис. 4. Главное окно панели администрирования системы Терминус

СПИСОК ЛИТЕРАТУРЫ

1. Руководящий документ. URL: http://fstec.ru/ (дата обращения: 19.10.2015).
2. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». М.: ГТК, 1992.
3. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». М.: ГТК, 1992.

Поступила в редакцию 30 ноября 2015 г.

Крючин Олег Владимирович, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, кандидат технических наук, ведущий программист института математики, естествознания и информационных технологий, e-mail: kryuchov@gmail.com

Рыбаков Михаил Анатольевич, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, магистрант по направлению подготовки «Прикладная математика и информатика» института математики, естествознания и информационных технологий, e-mail: kafedra_kmm@mail.ru

UDC 004.9
DOI: 10.20310/1810-0198-2016-21-1-146-149

DATA PROTECTION SYSTEM TERMINUS

© O.V. Kryuchin, M.A. Rybakov

Data protection system Terminus, which was aimed at protection data from unsanctioned access is described. This protection includes mandate and discrete division.
Key words: mandate access; discrete access; data protection.

REFERENCES

1. *Rukovodyashchiy dokument*. Available at: http://fstec.ru/ (accessed 19.10.2015).
2. *Rukovodyashchiy dokument Gostekhkomissii Rossii «Sredstva vychislitelnoy tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii».* Moscow, FSTEC of Russia Publ., 1992.
3. *Rukovodyashchiy dokument Gostekhkomissii Rossii «Zashchita ot nesanktsionirovannogo dostupa k informatsii. Terminy i opredeleniya»*. Moscow, FSTEC of Russia Publ., 1992.

Received 30 November 2015

Kryuchin Oleg Vladimirovich, Tambov State University named after G.R. Derzhavin, Tambov, Russian Federation, Candidate of Technics, Leading Programmer of Mathematics, Natural Science and Information Technologies Institute, e-mail: kryuchov@gmail.com

Rybakov Mikhail Anatolyevich, Tambov State University named after G.R. Derzhavin, Tambov, Russian Federation, Candidate for Master's Degree of Preparation Direction "Applied Mathematics and Informatics" of Mathematics, Natural Science and Information Technologies Institute, e-mail: kafedra_kmm@mail.ru