УДК 681.3.07

*А.В. Головин, В.В. Поляков, В.П. Каракулин*

# Реализация модели ролевого разграничения доступа для автоматизированного рабочего места пользователя

Современные информационные технологии требуют особого сопровождения с точки зрения безопасности. Требования безопасности обычно сводятся к многофакторной идентификации и аутентификации пользователя для его авторизации в системе [1, 2], например, на основе алгоритма прохода по двум ключам [3]. Аутентификация пользователя требует ввода пароля с клавиатуры, причем система оказывается защищенной лишь в случае пароля, состоящего из случайных символов [4]. Такой пароль тяжело запоминается, поэтому фиксируется на бумаге, что резко повышает возможность его компрометации, и, как следствие, повышается вероятность несанкционированного доступа к системе.

Работа еще больше усложняется, если потребовать использование автоматизированного рабочего места другим пользователем, но с тем же самым кругом обязанностей, например, когда основной пользователь в командировке, отпуске и др. Тем не менее удается сохранить требуемый уровень безопасности без усложнения сопровождения компьютерной системы, если реализовать авторизацию пользователя по ключу на основе расписания, в котором для заданного интервала времени жестко назначать определенный компьютер для данного пользователя, выступающего в фиксированной роли.

В статье предлагается компьютерный программно-аппаратный комплекс, созданный на базе стандартных автоматизированных рабочих мест пользователя, дополненный авторизацией по идентификатору на основе ключа из USB FLASH-устройства, в котором реализована модель ролевого разграничения доступа, управляемая по расписанию.

Компьютерная система состоит из сервера, содержащего расписание, и клиентских компьютеров. Каждый клиент представляет собой автоматизированное рабочее место пользователя на основе Linux, дополненное пакетами ролевого разграничения доступа RSBAC и управления доступом для графической оболочки.

Процедура работы авторизации в автоматизированном рабочем месте происходит следующим образом. На этапе загрузки операционной системы и активации демона графической подсистемы USB FLASH-устройство, выполняющее функции ключа доступа, должно быть подключено к компьютеру. В этом случае происходит чтение идентификатора и строки записи расписания из защищенной области ключа. Если USB FLASH-устройство не подключено к компьютеру, то система просит выполнить обычную процедуру идентификации и аутентификации с клавиатуры, что может потребоваться для целей администрирования.

Строка записи расписания содержит доступный интервал времени для работы пользователя, включающий текущее время, идентификатор компьютера на основе MAC-адреса и список доступных ролей для пользователя.

Расписание, состоящее из строк записи, создается и сопровождается на сервере администратором безопасности, синхронизация клиентской копии части расписания, относящейся к этому ключу (и, соответственно, пользователю), происходит по инициативе сервера при очередном удачном подключении USB FLASH-устройства к компьютеру по истечении фиксированного интервала времени обновления. Разметку USB FLASH-устройства проводит администратор безопасности при помощи специализированной утилиты сервера единовременно при создании нового пользователя.

Использование такой системы безопасности приводит к тому, что пользователь может авторизоваться только на том компьютере, во время того интервала времени и с той ролью, которая указана в расписании.

Во время работы пользователя проводится постоянный контроль наличия подключенного USB FLASH устройства. При отключении устройства сеанс пользователя завершается.

Компьютерная система реализована при помощи свободного программного обеспечения независимых разработчиков, что позволяет получить максимальный уровень контроля кода.

Мандатный контроль доступа в рамках модели Белла-ЛаПадула [5, 6] выполнен на основе пакета RSBAC. Rule Set Based Access Control (RSBAC) [7] поддерживает набор современных моделей безопасности и дает легко расширяемое, полностью контролируемое по доступу управление пользователями на уровне ядра операционной системы. Мандатное разграничение доступа дополнено ролевой моделью и обычными списками доступа, унаследованными от дискреционной модели разграничения доступа [8]. На основе пакета на уровне ядра операционной системы активированы модули:

- MAC (Mandatory Access Control) обеспечивает мандатный контроль доступа [9];
- FF (File Flags) управляет правами доступа на каталоги и наследование таких прав доступа;
- ACL (Access Control Lists) задает дискреционное разграничение доступа [8] на основе списков доступа;
- RC (Role Compatibility) определяет ролевое разграничение доступа для ролей и типов [6, 9], представляющих собой абстрактные объекты для описания пользователей, программ и файлов.

Синхронизация части расписания, принадлежащей пользователю, и расписания клиента осуществляется при помощи алгоритмов, реализованных на основе пакета rsync [10–12].

Разработанная компьютерная система предлагается для реализации многофакторной идентификации и аутентификации пользователя по расписанию и ролевого разграничения доступа для компьютеров, выполняющих роль автоматизированных рабочих мест, в том числе как основа автоматизированных рабочих мест для учреждений образования.

## Библиографический список


1. Шрамко, В.Н. Комбинированные системы идентификации и аутентификации / В.Н. Шрамко // PCWeek/RE. – 2004. – №45.
2. Головин, А.В. Частично контролируемая компьютерная система для критических приложений / А.В. Головин, В.В. Поляков, В.П. Каракулин // Известия АлтГУ. – Барнаул, 2007. – №1.
3. Омельянчук, А.М. Усиленные алгоритмы в системах доступа особо важных объектов / А.М. Омельянчук // Системы безопасности. – 2005. – №2.
4. Смит, Р.Э. Аутентификация: от паролей до открытых ключей / Р.Э. Смит. – М., 2002.
5. Bell, D.E. Secure Computer Systems: Unified Exposition and Multics Interpretation / D.E. Bell, L.J. LaPadula. – Bedford, 1976.
6. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М., 2000.
7. Rule Set Based Access Control (RSBAC) [Электронный ресурс] / Режим доступа: http://www.rsbac.org/, свободный. – Яз. англ.
8. Девянин, П.Н. Теоретические основы компьютерной безопасности / П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. – М., 2000.
9. Sandhu, R. Role-Based Access Control, Advanced in Computers / R. Sandhu. – 1998. – Vol. 46.
10. Rsync [Электронный ресурс] / Режим доступа: http://rsync.samba.org/, свободный. – Яз. англ.
11. Шредер, К. Rsync – современная стратегия архивирования информации / К. Шредер // Сетевые решения. – 2003. – №2. [Электронный ресурс] / Режим доступа: http://www.nestor.minsk.by/sr/2003/02/30209.html, свободный. – Яз. рус.
12. Tridgell, A. Efficient Algorithms for Sorting and Synchronization. A thesis submitted for the degree of Doctor of Philosophy at The Australian National University. February 1999. [Электронный ресурс] / Режим доступа: http://samba.org/~tridge/phd_thesis.pdf, свободный. – Яз. англ.