УДК 681.3.07

А.В. Головин, В.В. Поляков, С.А. Лапин

Ролевое разграничение доступа для автоматизированного рабочего места пользователя при оперативном удаленном управлении конфиденциальной информацией

Рассматривается компьютерная система, использующая ролевое разграничение доступа, позволяющая выполнять аутентификацию пользователя, безопасную синхронизацию конфиденциальных данных, разграничение доступа пользователей при работе с изменяемой информацией на удаленном компьютере автоматизированной системы, управляемой с сервера в головной организации.
Ключевые слова: автоматизированное рабочее место, аудит, синхронизация, ролевое разграничение доступа.

При проведении аудита удаленных филиалов распределенных организаций выдвигаются повышенные требования к защите информации, особенно в случае слабой пропускной способности или низкого качества каналов связи. Для защиты информации обычно используются многофакторная идентификация и аутентификация пользователя для его авторизации в системе [1, 2, 6]. Тонкую настройку разграничения уровней доступа к конфиденциальной информации обычно реализуют на основе ролевого разграничения доступа [3, 4]. Однако в случае смены пользователей и их ролей резко возрастает опасность компрометации ценной информации. Кроме того, остается нерешенным вопрос об оперативном изменении и синхронизации конфиденциальных данных, относящихся к пользователю.

В настоящей работе рассматривается компьютерная система, использующая ролевое разграничение доступа, свободная от указанных недостатков.

Такая система позволяет решать следующие задачи: аутентификация пользователя; безопасная синхронизация конфиденциальных данных; разграничение доступа пользователей при работе с частично изменяемой информацией на удаленном компьютере автоматизированной системы, управляемой с сервера в головной организации.

Предлагаемая компьютерная система (рис. 1) состоит из сервера (включенного в локальную сеть головной организации), связанного с удаленными подсетями филиалов организации при помощи компьютерной сети. Поскольку дополнительных требований безопасности к сети связи не предъявляется, это может быть сеть Интернет. Сервер хранит базу данных с учетными записями пользователей (логины и пароли), а также список доступных пользователям ролей. Такую базу данных назовём базой данных пользователей и ролей, а информацию, отнесенную к одному пользователю, выступающему в текущей роли, назовем текущей записью пользователя.

На этапе загрузки операционной системы на клиентском компьютере происходит синхронизация базы данных пользователей и ролей. Для этого используется модифицированный протокол rsync [5], работающий в защищенном режиме с использованием криптографических методов при обмене информацией [4]. Главная изменяемая администратором безопасности база данных пользователей и ролей филиала расположена на сервере головной организации.

На клиентский компьютер по защищенному каналу передаются лишь изменения, внесённые на сервере головной организации. Возможность изменения базы данных пользователей и ролей в филиале исключается.

Ролевое разграничение доступа реализовано на основе пакета RSBAC (Rule Set Based Access Control), в частности, с использованием его модуля RC, определяющего правила ролевого разграничения доступа [4]. Использование такой системы приводит к тому, что на клиентском компьютере пользователь может авторизоваться только если ему разрешено в это время находиться в данном филиале по своим служебным обязанностям (ограничение по времени) и только с той ролью, что соответствует хранящейся в базе данных пользователей и ролей.

Процедура аутентификации пользователя на автоматизированном рабочем месте происходит следующим образом. Сотрудник, роль которого подходит, чтобы воспользоваться ресурсами данного автоматизированного рабочего места в режиме аудита, подключает свой USB FLASH. В этом случае происходит чтение идентификатора и пароля FLASH-устройства, который сверяется с извлеченным из синхронизованной базы данных поль-

зователей и ролей. При успешном окончании этой операции система просит пользователя выполнить дополнительную процедуру аутентификации с клавиатуры путем ввода пароля пользователя, что исключает компрометацию идентификатора на USB FLASH-устройстве, в том числе вследствие его утраты.

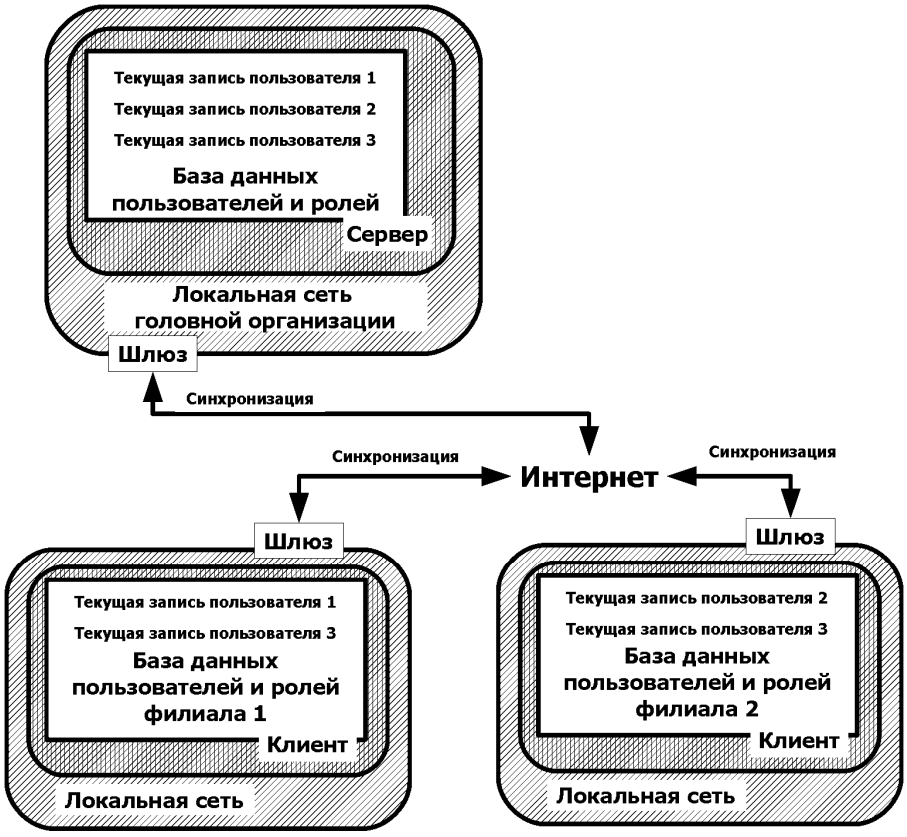

Рис. 1. Защищенная компьютерная система

Разметку USB FLASH-устройства проводит администратор безопасности при помощи специализированной утилиты сервера единовременно при создании нового пользователя.

Успешная аутентификация пользователя приводит к авторизации его в системе. При этом пользователю становится доступна лишь защищенная папка на компьютере. В ней могут сохраняться введенные с клавиатуры документы. После авторизации и в процессе завершения сеанса работы в системе происходит синхронизация этой защищенной папки с информацией в базе данных на сервере головной организации. Процедура выполняется во временных рамках, заданных расписанием работы пользователя [4]. Временные рамки задаются указанием даты и времени начала и конца, соответственно, легитимности текущей записи пользователя и являются часть такой записи в базе данных пользователей и ролей. При первом разрешенном входе пользователя защищенная папка создается, вне временных рамок при старте системы защищенная папка удаляется.

Предложенная защищенная компьютерная система, включающая сервер головной организации и набор автоматизированных рабочих мест пользователя в каждом удаленном филиале, позволяет повысить надежность защиты часто изменяемой информации и представляется эффективной для проведении аудита филиалов в распределенной организации.

Литература

1. Шрамко В.Н. Комбинированные системы идентификации и аутентификации // PCWeek / RE. – 2004. – № 45 [Электронный ресурс]. – Режим доступа: http://daily.sec.ru/dailypblshow.cfm?rid=5&pid=12928&pos=4&stp=25&cd=13&cm=4&cy=2010,свободный (дата обращения: 21.05.2010).

2. Омельянчук А.М. Усиленные алгоритмы в системах доступа особо важных объектов // Системы безопасности. – 2005. – № 2. – С. 116–120.

3. Головин А.В. Частично контролируемая компьютерная система для критических приложений / А.В. Головин, В.В. Поляков, В.П. Каракулин // Известия АлтГУ (Барнаул). – 2007. – № 1. – С. 52–54.

4. Головин А.В. Реализация модели ролевого разграничения доступа для автоматизированного рабочего места пользователя / А.В. Головин, В.В. Поляков, В.П. Каракулин // Известия АлтГУ (Барнаул). – 2009. – № 1. – С. 91–92.

5. 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. – 106 p.

6. Мещеряков Р.В. Специальные вопросы информационной безопасности / Р.В. Мещеряков, А.А. Шелупанов. – Томск: Изд-во Ин-та оптики атмосферы СО РАН, 2003. – 224 с.

Головин Александр Витальевич
Канд. физ.-мат. наук, доцент каф. прикладной физики, электроники и информационной безопасности Алтайского государственного университета (АлтГУ), г. Барнаул
Тел.: (+7-385-2) 36-48-09
Эл. адрес: gav162@yandex.ru

Поляков Виктор Владимирович
Доктор физ.-мат. наук, профессор каф. прикладной физики, электроники и информационной безопасности АлтГУ, г. Барнаул
Тел.: (+7-385-2) 36-48-09
Эл. адрес: pvv@asu.ru

Лапин Сергей Александрович
Аспирант каф. прикладной физики, электроники и информационной безопасности АлтГУ, г. Барнаул

A.V. Golovin, V.V. Polyakov, S.A.Lapin

Role differentiation of access for the user automated workplace at operative remote control of the confidential information

In work considered computer system, using role based access control and allowing perform user autentification, security synchronization confidential data, user access control for work width change information on remote computer in automatic system which controlled width server main organization.
Keywords: automated workstation, audit, synchronization, role based access control.
