УДК 004.056.53

Т. С. Осадчая, инженер, e-mail: taniaosadchaya6@gmail.com, **А. Ю. Щеглов**, д-р техн. наук, проф.,
Университет ИТМО, Санкт-Петербург, Россия

Комплексное решение задачи защиты от атак с правами привилегированного пользователя

Работа посвящена решению задачи комплексной защиты от атак с правами привилегированного пользователя. Рассматриваются следующие источники данной угрозы безопасности: легальные пользователи, имеющие привилегированные права, и вредоносные программы, запущенные с привилегированными правами. Рассмотрен подход, обеспечивающий контроль и усечение действий привилегированных пользователей, в том числе усечение их возможностей по администрированию, а также исключение возможности влияния вредоносных программ, запущенных с привилегированными правами, на систему.

Ключевые слова: *привилегированные пользователи, инсайдеры, контроль доступа, права доступа, усечение возможностей пользователей по администрированию, механизм самозащиты, вредоносная программа*

Введение

В настоящее время одной из актуальных угроз безопасности является наличие привилегированных прав, поскольку привилегированные пользователи имеют доступ к важным, имеющим стратегическое значение, данным, а также к конфиденциальной информации о компании или ее сотрудниках [1].

Существуют два *источника* этой угрозы безопасности:

- действия пользователя, имеющего привилегированные права (например, системного администратора);
- запуск тем или иным образом вредоносной программы, предполагающей некое воздействие на систему, с привилегированными правами.

Необходимо отметить, что привилегированный пользователь является одним из самых опасных инсайдеров — внутренних пользователей, которые преднамеренно или случайно могут допустить утечку конфиденциальной информации [2, 3].

В случае неправомерных действий пользователей, обладающих привилегированными правами, может быть нанесен серьезный ущерб, так как такие пользователи имеют доступ к системным настройкам, управлению пользователями и управлению разрешениями, т. е. имеют широкий доступ к критически важным приложениям, ключевым системам и информации [4].

Сегодня средством любой атаки, в частности целевой, направленной против конкретной компании или государственного органа и предполагающей использование уязвимостей в различных программных средствах, является запуск какой-либо сторонней вредоносной программы с правами привилегированного пользователя. Исследования показывают, что 80 % целевых атак предполагают взлом привилегированной учетной записи [5].

Следовательно, ***задачами средств защиты информации*** являются:

- контроль привилегированных пользователей и возможность воздействия на их права в целях снижения вероятности осуществления данными пользователями инсайдерской атаки;
- предотвращение влияния программ, запущенных с привилегированными правами, на систему.

Поскольку в основе архитектуры защиты современных универсальных операционных систем (в частности, систем семейств Windows и Unix) лежит принцип "полного доверия к администратору", их встроенные механизмы защиты не могут обеспечить эффективного противодействия внутренним угрозам: ими не предоставляются возможности отслеживания и защиты от действий привилегированных пользователей [6]. Следовательно, контроль действий привилегированных пользователей возможен только по-

средством применения специализированных решений — средств контроля привилегированных пользователей.

Указанные выше задачи необходимо решать в комплексе. Необходимо как контролировать и разграничивать права доступа привилегированного пользователя (администратора), так и предотвращать возможность влияния на систему программ, которые могут быть наделены вредоносными свойствами и запущены под привилегированной учетной записью.

Для этого субъект доступа должен содержать два компонента: "учетная запись" и "процесс". Кроме того, защита, связанная с усечением и контролем прав доступа, должна решаться на системном уровне для противодействия любому воздействию привилегированных пользователей на систему защиты (удаление, останов служб и т. д.).

В настоящее время развито направление, связанное с контролем действий привилегированных пользователей. Англоязычными аналогами наименования решений по управлению привилегированными пользователями являются Privileged User Management (PUM), Privileged Identity Management (PIM) и др. [7].

Принцип работы средств контроля привилегированных пользователей представляет собой проверку и подтверждение полномочий привилегированных пользователей, выявление их подозрительной активности с помощью регистрации всех действий, уведомление ответственных лиц о такой активности и при необходимости принудительный разрыв сессии.

Основными задачами, решаемыми средствами контроля привилегированных пользователей, являются:

- централизованное управление привилегированными учетными записями, автоматическое обнаружение привилегированных учетных записей;
- управление аутентификацией и авторизацией (включая управление парольной защитой) для привилегированных учетных записей для точной идентификации пользователя, работающего под учетной записью администратора в конкретный момент времени;
- аудит действий, выполняемых привилегированными пользователями (определение времени обращения к конфиденциальным данным и имени пользователя, ведение журнала выполненных действий, их отслеживание в режиме реального времени), в том числе видеофиксация всех подключений и сессий;
- создание политик доступа для привилегированных пользователей к корпоративным ресурсам (типы сеансов, протоколы доступа, время доступа и т.п.), так данные пользователи получат только необходимый и достаточный доступ к обслуживаемым информационным системам.

Таким образом, существующие в настоящее время решения, посвященные контролю действий привилегированных пользователей, реализуются внешними средствами и в первую очередь ориентированы на задачи контроля привилегированных пользователей [8, 9].

В составе подавляющей части существующих PUM-решений отсутствуют клиентская часть и собственные драйверы. Как следствие, данные решения могут реализовывать только настройку встроенных возможностей операционной системы, при этом средство защиты становится "шлюзом" между машиной администратора и целевой машиной для контроля действий привилегированных пользователей.

PUM-решения ставят своей основной целью регистрацию всех действий привилегированных пользователей для их дальнейшего анализа. Однако данными средствами не решается в полной мере задача по усечению возможностей пользователей, имеющих повышенные привилегии, по администрированию. Также в них отсутствует защита от целевых атак, более того, вносится дополнительная угроза уязвимости самого PUM-решения.

Комплексная система защиты информации "Панцирь+" для ОС Microsoft Windows (КСЗИ "Панцирь+") на сегодняшний день является единственной системой, в которой субъект доступа идентифицируется парой "пользователь — процесс". Данная возможность является запатентованной [10]. При этом КСЗИ работает на системном уровне и запускается как системная служба, права которой выше, чем права администратора. КСЗИ "Панцирь+" решает задачи, отличные от задач PUM-решения, что позволяет апробировать предлагаемый в данной статье подход к защите.

Целью исследования является повышение уровня безопасности и сохранение конфиденциальности и целостности системных объектов, настроек операционной системы и данных пользователей.

Основными задачами, решаемыми в комплексе в рамках реализации этой цели, являются:

контроль и усечение действий легальных привилегированных пользователей;

предотвращение влияния на систему вредоносных программ, запущенных с привилегированными правами.

Идея подхода к защите заключается в необходимости:

- создания разграничительной политики доступа для пользователей с привилегированными правами;

- исключения возможности воздействия любыми сторонними программами на системные объекты и объекты, хранящие данные.

Необходимо отметить, что данный подход базируется на реализации механизма самозащиты, обеспечивающего невозможность влияния на функционирование средства защиты информации привилегированными пользователями любым способом. Данный механизм не позволит привилегированному пользователю, не являющемуся администратором безопасности, каким-либо образом повлиять на запущенную службу и драйверы средства защиты, модифицировать его настройки.

Кроме того, средством защиты должны реализовываться два уровня иерархии администраторов: администратор безопасности и остальные привилегированные пользователи. Администратор безопасности определяет права других привилегированных пользователей, разрешая им требуемый набор функций администрирования из предоставленных операционной системой. Средством защиты при этом может управлять только администратор безопасности. Без реализации подобной иерархии осуществить усечение прав пользователей, имеющих повышенные привилегии, невозможно.

Контроль и усечение действий легальных привилегированных пользователей

В общем случае задача защиты информации от привилегированных пользователей заключается в том, чтобы данные пользователи (например, системные администраторы) не имели доступа к файлам, создаваемым другими пользователями [11]. Данная задача решается благодаря созданию разграничительной политики доступа с использованием механизма контроля доступа к создаваемым файлам. Основу контроля доступа к создаваемым файлам составляет их автоматическая разметка. При создании субъектом нового файла он автоматически размечается: им наследуется учетная информация субъекта доступа, создавшего этот файл [12]. Используя данный механизм, можно задать такие правила, что привилегированный пользователь будет иметь доступ только к тем файлам, которые были созданы им.

Для контроля действий привилегированных пользователей необходимо настроить параметры аудита, задав объекты, доступ к которым будет регистрироваться в журналах аудита.

Существуют следующие виды контроля действий:

- контроль отказов — в аудите отображаются выполненные пользователем действия, которые запрещены ему разграничительной политикой (рис. 1);
- контроль действий — в аудите отображаются выполненные пользователем действия (рис. 2).

Кроме того, возможна локализация аудита: благодаря настройке параметров аудита можно контролировать не все действия привилегированных пользователей, а, например, только работу с различными оснастками панели управления, редактирование автозагрузки, повышение привилегий.

Для усечения возможностей привилегированных пользователей по администрированию следует использовать подход, основанный на разрешении доступа к защищаемому объекту файловой системы или реестра только соответствующей библиотеке, которая включает в себя интерфейс настройки. Таким образом, создается разграничительная политика для процессов, после чего привилегированному пользователю разрешается либо запрещается запуск данной библиотеки.

В рамках данного подхода сначала выбирается требуемая функция администрирования, после

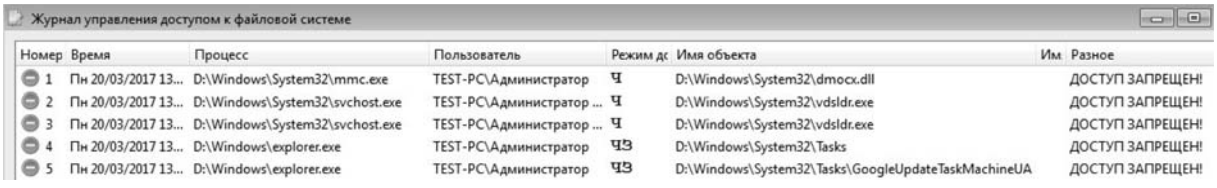

Рис. 1. Пример аудита (контроль отказов)

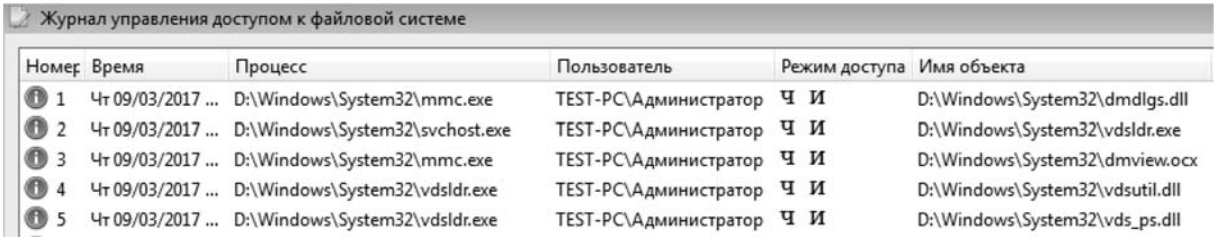

Рис. 2. Пример аудита (контроль действий)

чего определяется библиотека или исполняемый файл, с помощью которого возможна работа с определенным интерфейсом, связанным с выполнением рассматриваемой функции.

Затем обеспечивается возможность осуществления записи только из выбранного интерфейса: осуществлять запись в защищаемый объект файловой системы или реестра должен только один определенный процесс, всем остальным процессам запись в данный объект запрещается.

После этого при создании разграничительной политики для привилегированного пользователя ему разрешается или запрещается запуск этой библиотеки или исполняемого файла.

Примеры разграничительных политик, используемые далее в данной работе, были созданы с использованием КСЗИ "Панцирь +" для ОС Microsoft Windows.

Пример разграничительной политики для защиты от действий легальных привилегированных пользователей

Были заданы правила доступа привилегированному пользователю к создаваемым файлам, которые запрещают ему доступ к файлам, созданным и обрабатываемым интерактивными пользователями (рис. 3).

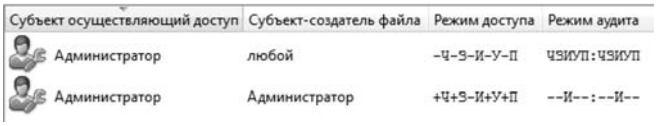

Рис. 3. Пример разграничительной политики доступа к создаваемым файлам

Примеры разграничительных политик

Возможность по администрированию	Объект	Права доступа
Открытие элемента панели управления "Учетные записи пользователей"	C:\Windows\System32\usercpl.dll	−И
Отображение вкладки "Безопасность" в свойствах папок и файлов	C:\Windows\System32\authz.dll	−И
Открытие элемента панели управления "Дата и время"	C:\Windows\System32\timedate.cpl; HKLM\System\CurrentControlSet\Control\TimeZoneInformation; HKLM\SYSTEM\ControlSet001\Control\TimeZoneInformation	−И; +Ч−З−У−П; +Ч−З−У−П

В результате реализации данной разграничительной политики привилегированный пользователь сможет иметь доступ только к файлам, созданным им. При этом ему запрещено запускать созданные им исполняемые файлы.

Благодаря запрету на запуск соответствующих динамических библиотек были усечены возможности привилегированного пользователя по администрированию.

Рассмотрим примеры политик безопасности, соответствующих усечению различных возможностей привилегированных пользователей по администрированию. Ниже представлены правила, относящиеся к привилегированным пользователям. До их создания необходимо сначала запретить любым процессам чтение/исполнение требуемых динамических библиотек или исполняемых файлов, а также запретить запись в соответствующие объекты файловой системы и реестра. Примеры разграничительных политик представлены в таблице.

Здесь "−И" — запрет на исполнение, "+Ч" — разрешение на чтение, "−З" — запрет на запись, "−У" — запрет на удаление, "−П" — запрет на переименование.

В результате реализации данных разграничительных политик (рис. 4—6) Администратор не сможет открыть элемент панели управления

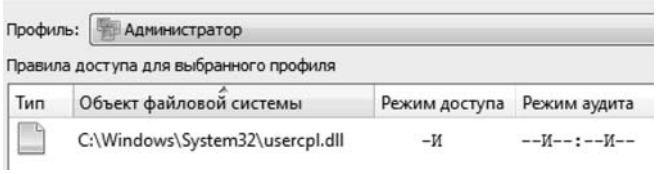

Рис. 4. Пример разграничительной политики (открытие элемента панели управления)

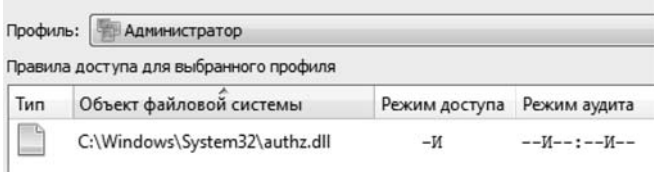

Рис. 5. Пример разграничительной политики (отображение вкладки "Безопасность")

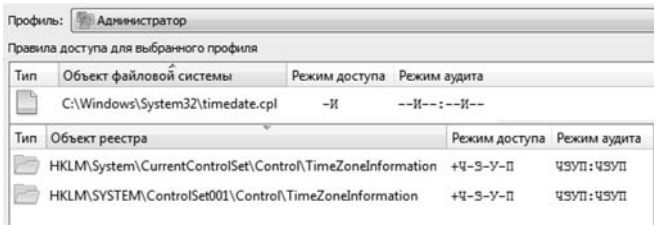

Рис. 6. Пример разграничительной политики (открытие элемента панели управления)

"Учетные записи пользователей", увидеть вкладку "Безопасность", открыв свойства какой-либо папки или файла, открыть элемент панели управления "Дата и время".

Исключение возможности влияния на систему вредоносной программы, запущенной с привилегированными правами

Реализация рассматриваемого подхода к защите состоит в выборе объектов, запись в которые позволена только определенным процессам. При этом должна предотвращаться возможность их модификации любыми другими процессами.

Рассматриваемые подходы реализованы на практике и апробированы при построении комплексной системы защиты информации "Панцирь+" для ОС Microsoft Windows.

Пример разграничительной политики для защиты от влияния на систему вредоносных программ, запущенных с привилегированными правами

Был выбран объект "%SystemRoot %\system32*"; всем процессам, находящимся в директории "%SystemRoot%\system32*", был предоставлен полный доступ к данному объекту; всем остальным процессам (используется маска "*") модификация выбранного объекта была запрещена (т.е. им разрешается только чтение и исполнение объектов, находящихся в выбранной директории).

Таким образом, в разграничительной политике были созданы следующие правила (рис. 7).

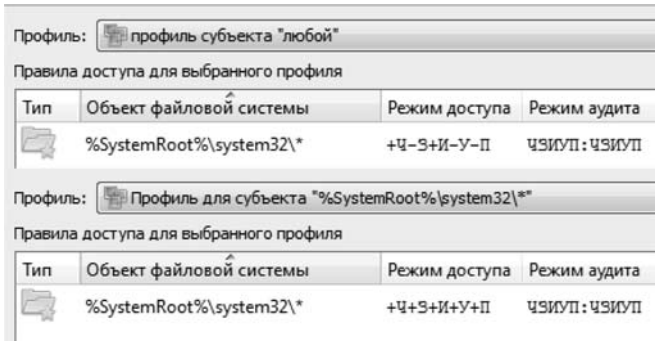

Рис. 7. Пример разграничительной политики для защиты от влияния вредоносных программ: "Ч" — чтение, "З" — запись, "И" — исполнение, "У" — удаление, "П" — переименование

В результате реализации данной разграничительной политики любая сторонняя программа не будет иметь возможности провести запись или модификацию выбранных объектов.

Рассмотрим следующий пример: пусть некая программа Procmon64.exe запущена с правами привилегированного пользователя в целях изменения выбранных файлов.

Поскольку данная программа не расположена в директории "%SystemRoot%\system32", при обращении ее к объектам, находящимся в указанной выше директории, возможность влияния данной программой на систему будет исключена. В журнале контроля действий появятся сообщения, представленные на рис. 8.

Заключение

Подводя итог, следует отметить, что в результате осуществления рассмотренного подхода к реализации разграничительной политики при определенных условиях поставленные задачи могут быть решены эффективно. Удается не только защитить информацию, обрабатываемую на компьютере, от привилегированных пользователей и усечь возможности данных пользователей по администрированию, но и исключить возможность влияния на систему вредоносных программ, запущенных с привилегированными правами. При реализации рассматриваемого подхода возможности привилегированного пользователя будут определяться системой защиты, а любая сторонняя программа не будет иметь возможности провести запись или модификацию выбранных системных объектов.

Рассматриваемое решение было апробировано при разработке комплексной системы защиты информации "Панцирь+" для ОС Microsoft Windows.

Такое решение позволяет серьезно разграничить права привилегированных пользователей. Поэтому при использовании подобной системы актуальной становится задача защиты от повышения прав администратора до прав системы. Данный вопрос будет рассмотрен в следующей статье.

Список литературы

1. **Жан-Ноэль де Гальзан.** CEO WALLIX — Комплексная политика безопасности должна включать эф-

Рис. 8. Отказы в доступе

фективное управление привилегированными пользователями. URL: http://it-bastion.com/wp-content/uploads/2016/10/JN_interview_2013RU.pdf (дата обращения: 20 ноября 2017 г.).

2. **Беляева М., Синельников А.** Защита от инсайдеров — миф или реальность? // Information Security / Информационная безопасность. 2008. № 3.

3. **Угроза** привилегированных пользователей и методы по ее устранению. URL: http://ppt.ru/guide/news/136623 (дата обращения: 20 ноября 2017 г.).

4. **Сердюк В., Романов М.** Обратная сторона привилегий // BIS JOURNAL — Информационная безопасность банков. 2017. № 1.

5. **Крис Брук.** 88 % сетей уязвимы к взлому привилегированных аккаунтов. URL: https://threatpost.ru/88-percent-of-networks-susceptible-to-privileged-account-hacks/13219/ (дата обращения: 20 ноября 2017 г.)

6. **Щеглов А. Ю.** Компьютерная безопасность. Противодействие внутренним ИТ-угрозам. Часть 1. Угроза хищения данных с использованием мобильных накопителей. URL: http://www.npp-itb.spb.ru/publications/16.html (дата обращения: 20 ноября 2017 г.)

7. **Гридасов В.** Контроль привилегированных пользователей (PUM) — обзор мирового и российского рынка. URL: https://www.anti-malware.ru/reviews/privileged_user_management_market_russia_2016# (дата обращения: 20 ноября 2017 г.)

8. **Романов М.** Системы контроля привилегированных пользователей // Information Security / Информационная безопасность. 2015. № 4.

9. **Шабанов И.** Проблемы контроля привилегированных пользователей и их решение на примере Wallix AdminBastion. URL: http://www.anti-malware.ru/node/12023# (дата обращения: 20 ноября 2017 г.)

10. **Патент** на изобретение № 2534599 / Щеглов А. Ю., Щеглов К. А. Система контроля доступа к ресурсам компьютерной системы с субъектом доступа "пользователь, процесс".

11. **Щеглов А. Ю., Щеглов К. А.** Анализ и проектирование защиты информационных систем. Контроль доступа к компьютерным ресурсам. Методы, модели, технические решения. СПБ.: Профессиональная литература, 2017.

12. **Патент** на изобретение № 2524566 / Щеглов А. Ю., Щеглов К. А. Система контроля доступа к файлам на основе их автоматической разметки.

T. S. Osadchaya, Engineer, e-mail: taniaosadchaya6@gmail.com, **A. Yu. Shcheglov,** Ph. D., Professor,
ITMO University, St. Petersburg, Russia

Comprehensive Solution of Protection against Attack with Rights of Privileged Users

The work is dedicated to solvation of the problem of complex protection against attacks with privileged user rights. The following sources of this security threat are considered: legal users with privileged rights, and malicious programs running with privileged rights. The new approach of protection is described. It provides control and delineation of the actions of privileged users, including limitation of their administration capabilities, as well as excluding the possibility of the influence of malicious programs running with privileged rights on the system.

Keywords: *privileged users, insiders, access control, access rights, limitation of users' administration capabilities, self-defense mechanism, malicious software*

References

1. **Zhan-Nojel' de Gal'zan**, CEO WALLIX. Kompleksnaja politika bezopasnosti dolzhna vkljuchat' jeffektivnoe upravlenie privilegirovannymi pol'zovateljami. Available at: http://it-bastion.com/wp-content/uploads/2016/10/JN_interview_2013RU.pdf (accessed: 20 November 2017) (in Russian).

2. **Beljaeva M., Sinel'nikov A.** Zashhita ot insajderov — mif ili real'nost'? *Information Security*, 2008, no. 3, pp. 34—35 (in Russian).

3. **Ugroza** privilegirovannyh pol'zovatelej i metody po ejo ustraneniju. Available at: http://ppt.ru/guide/news/136623 (accessed: 20 November 2017) (in Russian).

4. **Serdjuk V., Romanov M.** Obratnaja storona privilegij. *BIS JOURNAL — Informacionnaja bezopasnost' bankov*, 2017, no. 1, pp. 32—33 (in Russian).

5. **Kris Bruk.** 88 % setej ujazvimy k vzlomu privilegirovannyh akkauntov. Available at: https://threatpost.ru/88-percent-of-networks-susceptible-to-privileged-account-hacks/13219/ (accessed: 20 November 2017) (in Russian).

6. **Shcheglov A. Yu.** Komp'juternaja bezopasnost'. Protivodejstvie vnutrennim IT-ugrozam. Chast' 1. Ugroza hishhenija dannyh s ispol'zovaniem mobil'nyh nakopitelej. Available at: http://www.npp-itb.spb.ru/publications/16.html (accessed: 20 November 2017) (in Russian).

7. **Gridasov V.** Kontrol' privilegirovannyh pol'zovatelej (PUM) — obzor mirovogo i rossijskogo rynka. Available at: https://www.anti-malware.ru/reviews/privileged_user_management_market_russia_2016# (accessed: 20 November 2017) (in Russian).

8. **Romanov M.** Sistemy kontrolja privilegirovannyh pol'zovatelej. *Information Security*, 2015, no.4, pp. 18—19 (in Russian).

9. **Shabanov I.** Problemy kontrolja privilegirovannyh pol'zovatelej i ih reshenie na primere Wallix AdminBastion. Available at: http://www.anti-malware.ru/node/12023# (accessed: 20 November 2017) (in Russian).

10. **Patent** na izobretenie № 2534599. Shcheglov A. Yu., Shcheglov K. A. Sistema kontrolja dostupa k resursam komp'juternoj sistemy s sub#ektom dostupa "pol'zovatel', process". (in Russian).

11. **Shcheglov A. Yu., Shcheglov K. A.** *Analiz i proektirovanie zashhity informacionnyh sistem. Kontrol' dostupa k komp'juternym resursam. Metody, modeli, tehnicheskie reshenija*. 2017. St.-Petersburg: Professional'naja literatura (in Russian).

12. **Patent** na izobretenie № 2524566. Shcheglov A. Yu., Shcheglov K. A. Sistema kontrolja dostupa k fajlam na osnove ih avtomaticheskoj razmetki (in Russian).