РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 390 839** (13) **C1**

(51) МПК
G06F 21/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2008143281/09, 23.10.2008**

(24) Дата начала отсчета срока действия патента:
23.10.2008

(45) Опубликовано: **27.05.2010** Бюл. № **15**

(56) Список документов, цитированных в отчете о поиске: **WO 02/097587 A2, 05.12.2002. RU 2308080 C2, 10.10.2007. WO 2006/124191 A1, 23.11.2006. US 2006/0026688 A1, 02.02.2006. US 2005/0246776 A1, 03.11.2005.**

Адрес для переписки:
195256, Санкт-Петербург, пр. Науки, 47, корп.2, кв.136, Д.П. Зегжде

(72) Автор(ы):
Абдульманов Роман Айдарович (RU),
Зегжда Дмитрий Петрович (RU),
Калинин Максим Олегович (RU)

(73) Патентообладатель(и):
ООО "НеоБИТ" (RU)

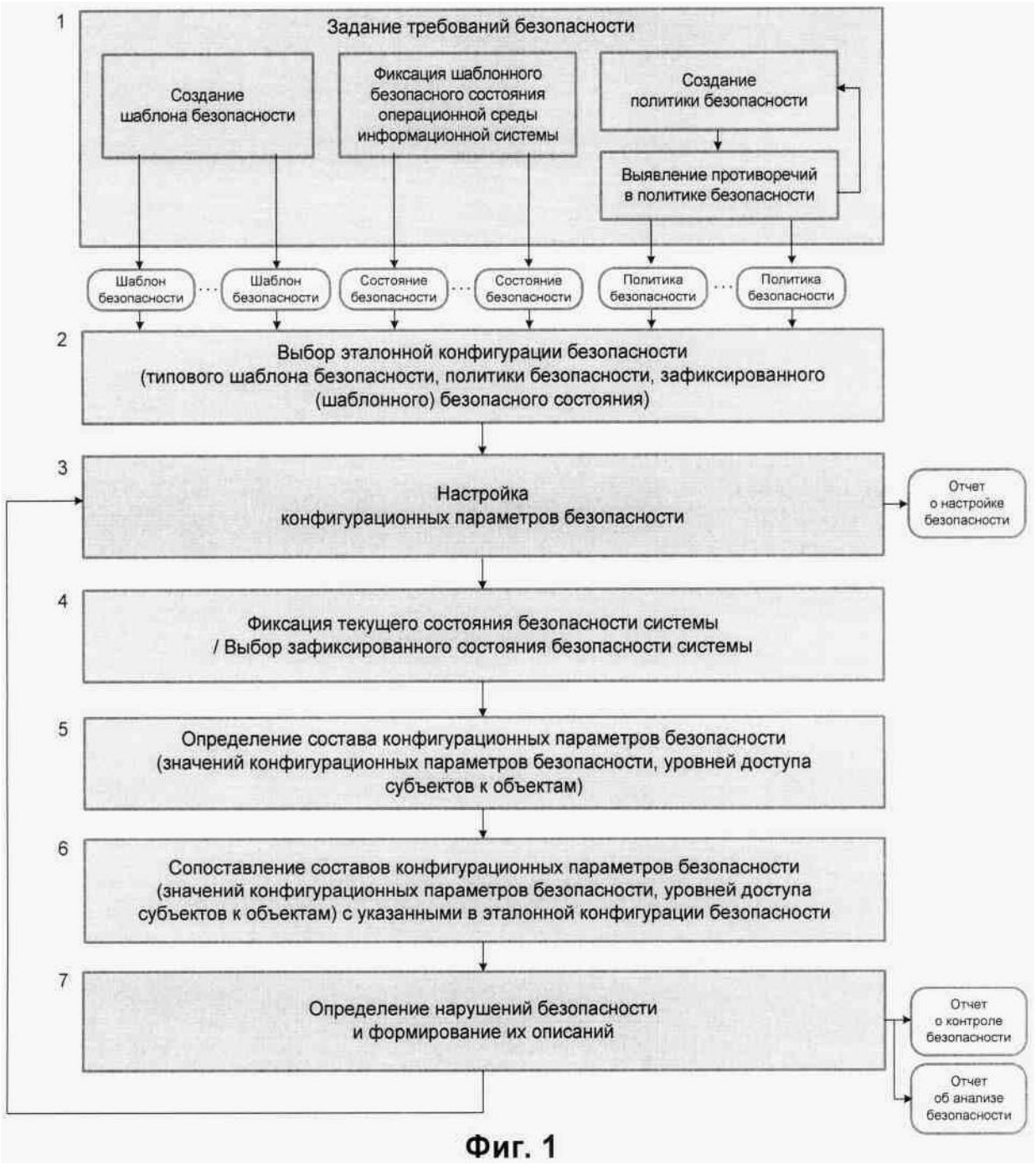
(54) СПОСОБ ЦЕНТРАЛИЗОВАННЫХ АВТОМАТИЗИРОВАННЫХ НАСТРОЙКИ, КОНТРОЛЯ И АНАЛИЗА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И СИСТЕМА ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ

(57) Реферат:

Изобретение относится к информационным системам и может быть использовано для управления информационной безопасностью, осуществляемого в автоматизированном режиме. Изобретение позволяет повысить эффективность обеспечения информационной безопасности и улучшить управляемость информационных систем. Изобретение предусматривает формирование типовых шаблонов и политик безопасности; выявление противоречий правил политик безопасности; настройку и фиксацию конфигурационных параметров безопасности в соответствии с заданными требованиями безопасности; контроль и анализ выполнения требований безопасности; выявление и описание связанных с конфигурационными параметрами нарушений безопасности и их составов; формирование инструкций по их устранению, устранение выявленных нарушений путем настройки конфигурационных параметров безопасности. При этом централизация, автоматизация и удаленное выполнение указанных процедур позволяет упростить процессы внедрения и мониторинга безопасности информационных систем, повысить результативность выявления и устранения ошибок администрирования, сократить ресурсо- и трудозатраты на поддержание информационной безопасности. 2 н. и 12 з.п. ф-лы, 3 ил.

RU 2390839 C1

RU 2390839 C1



Фиг. 1

RU 2390839 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 390 839** (13) **C1**

(51) Int. Cl.
G06F 21/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2008143281/09, 23.10.2008**

(24) Effective date for property rights:
23.10.2008

(45) Date of publication: **27.05.2010 Bull. 15**

Mail address:
195256, Sankt-Peterburg, pr. Nauki, 47, korp.2, kv.136, D.P. Zegzhde

(72) Inventor(s):
Abdul'manov Roman Ajdarovich (RU),
Zegzhda Dmitrij Petrovich (RU),
Kalinin Maksim Olegovich (RU)

(73) Proprietor(s):
OOO "NeoBIT" (RU)

(54) METHOD FOR CENTRALISED AUTOMATIC SETUP, MONITORING AND ANALYSING SECURITY OF INFORMATION SYSTEMS AND SYSTEM FOR IMPLEMENTING SAID METHOD

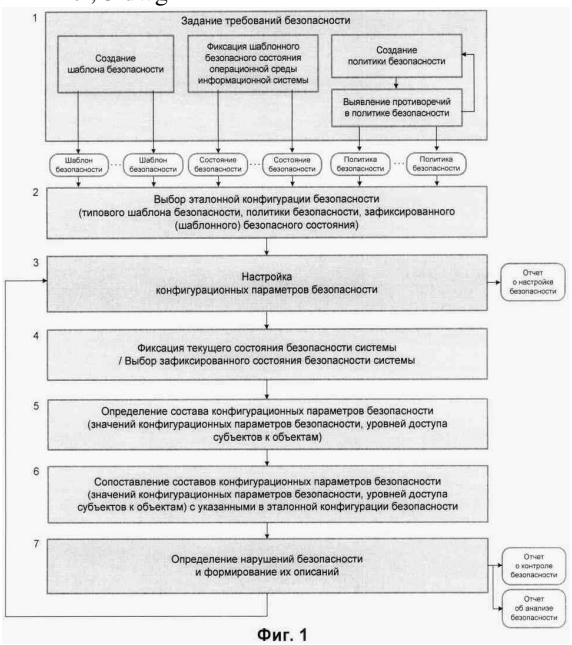
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention involves making standard templates and security policies; detecting contradictions in security policy rules; setting and fixing security configuration parametres in accordance with given security requirements; monitoring and analysis of meeting of security requirements; detection and description of security violations and their compositions related to parametre configurations; generating instructions for their elimination, elimination of detected violations by setting security parametre configurations. Centralisation, automation and remote execution of the said procedures simplifies the process of introducing and monitoring security of information systems, increases efficiency of detecting and correcting administration errors, cuts resource and labour inputs on maintaining information security.

EFFECT: more efficient maintenance of information security and improved manageability of information systems.

14 cl, 3 dwg



Фиг. 1

RU 2390839 C1

RU 2390839 C1

Изобретение относится к вычислительной технике, а именно к информационным системам, и может быть использовано для управления информационной безопасностью, осуществляемого в автоматизированном режиме путем централизованной настройки значений конфигурационных параметров безопасности операционных сред информационных систем; удаленной фиксации значений конфигурационных параметров безопасности операционных сред информационных систем; автоматического контроля и анализа безопасности текущей или предварительно зафиксированных системных конфигураций и выявления составов нарушений безопасности, вызванных ошибками, допущенными при администрировании; а также удаленного устранения выявленных нарушений безопасности.

Известны системы обеспечения информационной безопасности, например, WO 02097587, G06F, опубл. 2002-12-05; US 2005246776, H04L 9/00; G06F 11/30; G06F 12/14; H04L 9/32, опубл. 2005-11-03; EP 1784703, G06F 1/00; H04L 12/26; H04L 29/06, опубл. 2007-05-16; GB 2440697, G06F 21/00, опубл. 2008-02-06. Система, описанная в заявке WO 02097587, в своем составе содержит набор модулей сбора системных параметров, модуль проверки безопасности, а также совокупность блоков вывода информации, сетевого взаимодействия, управления компонентами и обеспечения безопасности системы.

Недостатки перечисленных систем заключаются в том, что ими выполняются только фиксированные проверки системных параметров, что делает невозможным контроль выполнения требований политик информационной безопасности. Кроме того, решения, представленные в этих патентах, основаны на принципе перебора фиксированного набора объектов и системных параметров. При этом не используются какие-либо аналитические модели или методы, вследствие чего не учитывается влияние косвенных зависимостей параметров на безопасность информационных систем, и, как следствие, не выявляются и не устраняются причины обнаруживаемых нарушений безопасности.

В основу изобретения положена задача создания способа централизованных автоматизированных настройки, контроля и анализа безопасности информационных систем и системы для его осуществления, которые предусматривают создание и редактирование типовых шаблонов безопасности; создание и редактирование политик безопасности; выявление противоречий правил разграничения доступа, составляющих политики безопасности; взаимодействие с программными средствами контроля и управления доступом операционной среды информационной системы; настройку и фиксацию конфигурационных параметров безопасности в соответствии с требованиями безопасности (типовыми шаблонами безопасности, построенными на основе рекомендаций по безопасной настройке операционной среды информационной системы; правилами разграничения доступа политик безопасности; зафиксированными (шаблонными) безопасными состояниями операционной среды информационной системы; правилами эффективного администрирования систем); контроль и анализ соответствия действующих и зафиксированных конфигурационных параметров безопасности требованиям безопасности (типовым шаблонам безопасности, построенным на основе рекомендаций по безопасной настройке операционной среды информационной системы; правилам разграничения доступа политик безопасности; зафиксированным (шаблонным) безопасным состояниям операционной среды информационной системы; правилам эффективного администрирования систем); выявление связанных с конфигурационными

параметрами нарушений безопасности (отклонений от типовых шаблонов безопасности; ошибок администрирования системных и пользовательских программ и ресурсов, допущенных при реализации политик безопасности; отклонений от зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы; проблем управления системой, заключающихся в неэффективном администрировании системы); определение конфигурационных параметров и их значений, составляющих каждое выявленное нарушение безопасности; формирование описаний выявленных нарушений безопасности и инструкций по их устранению; устранение выявленных нарушений путем настройки конфигурационных параметров безопасности в соответствии с сформированными инструкциями, что за счет централизации, автоматизации и удаленного выполнения процедур настройки, фиксации, контроля и анализа конфигурационных параметров безопасности позволяет значительно упростить процессы внедрения и мониторинга безопасности информационных систем, повысить результативность выявления и устранения ошибок администрирования, сократить ресурсо- и трудозатраты на поддержание информационной безопасности и тем самым повысить эффективность обеспечения информационной безопасности и улучшить управляемость информационных систем.

Решение этой задачи обеспечивается тем, что в способе централизованных автоматизированных настройки, контроля и анализа безопасности информационных систем создают типовой шаблон безопасности на основании рекомендаций по безопасной базовой настройке операционной среды информационной системы;

создают политику безопасности на основании требований безопасности, составляющих правила разграничения доступа субъектов к объектам;

при этом из каждой рекомендации, составляющей типовой шаблон безопасности, формируют критерий безопасности системы, представляемый в виде кортежей "Состав конфигурационных параметров безопасности" или "Значение конфигурационного параметра безопасности", описывающих условия, при соблюдении которых система является безопасной;

при этом из каждого правила разграничения доступа, составляющего политику безопасности, формируют критерий безопасности системы, представляемый в виде кортежа "Субъект-объект-уровень доступа", описывающего условие, при соблюдении которого система является безопасной;

в правилах разграничения доступа созданной политики безопасности производят поиск противоречий в указанных уровнях доступа субъектов к объектам с учетом иерархической структуры субъектов (отношений "группы пользователей - пользователи") и иерархической структуры объектов (отношений "контейнеры ресурсов - ресурсы") и в случае их обнаружения противоречий формируют описание противоречий, допущенных при задании правил разграничения доступа субъектов к объектам на разных уровнях иерархии субъектов и объектов, и производят коррекцию правил разграничения доступа соответствующей политики безопасности, исключая противоречивые правила или внося изменения в существующие правила и повторяя данную процедуру для всех правил до полного исключения противоречий;

из множества созданных типовых шаблонов и политик безопасности выбирают шаблон или политику, по которым должна быть выполнена настройка конфигурационных параметров безопасности, или на соответствие которым должны контролироваться конфигурационные параметры безопасности, или должна быть проанализирована безопасность системы;

при выполнении настройки конфигурационных параметров безопасности взаимодействуют с программными средствами контроля и управления доступом операционной среды информационной системы, выполняют установку значений конфигурационных параметров безопасности в соответствии с выбранным типовым шаблоном или политикой безопасности и составляют отчет о настройке безопасности, содержащий сведения об изменяемых конфигурационных параметрах безопасности и о результатах установки их значений;

при выполнении контроля или анализа конфигурационных параметров безопасности взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и фиксируют состав и действующие значения текущих конфигурационных параметров безопасности, формируя зафиксированное состояние безопасности информационной системы;

из множества зафиксированных состояний безопасности информационной системы выбирают состояние, на котором должны быть проконтролированы конфигурационные параметры безопасности или должна быть проанализирована безопасность системы;

на текущем или выбранном зафиксированном состоянии безопасности информационной системы контролируют и анализируют выполнение требований безопасности: типовых шаблонов безопасности, построенных на основе рекомендаций по безопасной настройке операционной среды информационной системы; правил разграничения доступа политик безопасности;

зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы; правил эффективного администрирования систем;

при этом в случае осуществления контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Состав конфигурационных параметров безопасности", если выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав зафиксированных конфигурационных параметров безопасности, и затем сравнивают множества зафиксированных конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, выявляют их различия и по результатам сравнения составляют отчет о контроле безопасности, содержащий описание выявленных отклонений от типового шаблона безопасности по составу конфигурационных параметров безопасности и инструкции по изменению состава конфигурационных параметров безопасности для устранения выявленных отклонений;

при этом в случае осуществления контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Значение конфигурационного параметра безопасности", если выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, и затем сравнивают

множества зафиксированных конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, сравнивают для подтвержденных конфигурационных параметров, указанных в выбранном типовом шаблоне безопасности и зафиксированных в системе, множества значений конфигурационных параметров безопасности с указанными в выбранном шаблоне или в политике безопасности, выявляют их различия и составляют отчет о контроле безопасности, содержащий описание выявленных отклонений от типового шаблона безопасности по составу и значениям конфигурационных параметров безопасности и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных отклонений;

при этом в случае осуществления анализа безопасности системы выполняют проверку соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в политике безопасности в виде кортежей "Субъект-объект-уровень доступа", если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, и затем сравнивают множества зафиксированных конфигурационных параметров безопасности с указанными в выбранной политике безопасности в части подмножеств субъектов и объектов, рассчитывают для всех подтвержденных пар "субъект-объект", указанных в выбранной политике безопасности и зафиксированных в системе, действующие уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех текущих зафиксированных конфигурационных параметров безопасности и их значений и затем сравнивают значения рассчитанных действующих уровней доступа с указанными в выбранном шаблоне или в политике безопасности, выявляя их различия, фиксируя состав и значения конфигурационных параметров, повлиявшие на отклонения уровней доступа, и составляя отчет об анализе безопасности, содержащий описание выявленных ошибок администрирования системных и пользовательских программ и ресурсов, допущенных при реализации политики безопасности, по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных нарушений и факторов влияния на уровни доступа;

при этом в случае осуществления анализа соответствия конфигурационных параметров безопасности зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы, если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, затем из множества ранее зафиксированных состояний безопасности информационной системы выбирают еще одно состояние, которое определяется как зафиксированное (шаблонное) безопасное состояние, после чего сравнивают текущие конфигурационные параметры

безопасности с указанными в зафиксированном (шаблонном) безопасном состоянии по составу и значениям, рассчитывают для всех подтвержденных пар "субъект-объект", указанных в выбранном зафиксированном (шаблонном) безопасном состоянии и зафиксированных в системе, действующие уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех текущих зафиксированных конфигурационных параметров безопасности и их значений, рассчитывают для тех же пар "субъект-объект" требуемые уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех конфигурационных параметров безопасности и их значений, указанных в зафиксированном (шаблонном) безопасном состоянии, сравнивают рассчитанные действующие и требуемые уровни доступа и составляют отчет об анализе безопасности, содержащий описание выявленных отклонений от зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных отклонений и факторов влияния на уровни доступа;

при этом в случае осуществления анализа соблюдения правил эффективного администрирования информационной системы, если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, оценивают по ним эффективность администрирования системы и объявляют ее эталонной, и после чего контролируют возникновение проблем управления системой, заключающихся в неэффективном администрировании системы, удаленно взаимодействуя со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируя состав и значения текущих конфигурационных параметров безопасности, оценивая по ним текущую эффективность администрирования системы, выполняя сравнение эталонного значения эффективности администрирования системы с текущим, определяя численные характеристики, снижающие эффективность администрирования системы, и составляя отчет об анализе безопасности, содержащий описание проблем управления системой, заключающихся в неэффективном администрировании системы, график изменения эффективности администрирования системы с течением времени, перечень численных характеристик, снижающих эффективность, и рекомендации по повышению эффективности администрирования системы;

с целью устранения выявленных нарушений безопасности производят настройку конфигурационных параметров безопасности в соответствии с инструкциями, сформированными в отчетах о контроле безопасности или в отчетах об анализе безопасности, и составляют отчет о настройке безопасности, содержащий сведения об изменяемых конфигурационных параметрах безопасности и о результатах установки их значений;

периодически повторяют в необходимой последовательности вышеуказанные действия по настройке, фиксации, контролю и анализу конфигурационных параметров безопасности, составляют множество отчетов о контроле, анализе и настройке

безопасности, тем самым непрерывно обеспечивая безопасность информационной системы.

В качестве состояния информационной системы рассматривают все множество конфигурационных параметров безопасности, а именно субъекты, объекты и их атрибуты безопасности, состав которых определяется типом операционной среды информационной системы. В общем случае состояние безопасности составляют такие конфигурационные параметры безопасности, как пользователи и группы пользователей; элементы файловой системы (диски, каталоги, файлы, ссылки), элементы реестра (разделы, ключи, параметры, ссылки); объекты ядра (задачи, процессы, потоки, драйверы, объекты синхронизации и т.д.); ресурсы общего доступа (каталоги, принтеры); программные сервисы; COM/DCOM-объекты; объекты службы каталога; локальные и глобальные настройки системной политики безопасности; опции и настройки безопасности пользовательского и специального программного обеспечения; конфигурационные параметры сетевых служб; атрибуты безопасности субъектов и объектов (идентификаторы защиты, привилегии пользователей и групп пользователей, информация о владельцах объектов, списки прав доступа, метки доступа и целостности, иерархическое распределение субъектов, объектов, прав доступа, меток доступа и целостности).

Типовые шаблоны безопасности составляют на основе рекомендаций экспертов по безопасной базовой настройке системных информационных ресурсов соответствующей операционной среды (Windows, UNIX и т.п.). Политики безопасности расширяют область действия типовых шаблонов безопасности за счет учета пользовательских информационных ресурсов помимо системных. Политики безопасности составляют на основе корпоративных требований контроля и управления доступом, предъявляемых к информационной системе, с учетом их выполнения в соответствующей операционной среде.

Каждая рекомендация, составляющая типовой шаблон безопасности, образует критерий безопасности системы, представляемый в виде кортежей "Состав конфигурационных параметров безопасности" или "Значение конфигурационного параметра безопасности", описывающих условия безопасности системы в виде множества конфигурационных параметров или их значений, соответственно.

Каждое правило разграничения доступа, составляющее политику безопасности, образует критерий безопасности системы, представляемый в виде кортежа "Субъект-объект-уровень доступа", описывающего отношение множеств субъектов, объектов и заданных для них уровней доступа, при выполнении которого система является безопасной. При составлении политики безопасности производят поиск противоречий в указанных уровнях доступа субъектов к объектам, определяя во множестве кортежей "Субъект-объект-уровень доступа" наличие ограничений, заданных для одной пары "субъект-объект", но с разными уровнями доступа, с учетом иерархической структуры субъектов (отношений "группы пользователей-пользователи") и иерархической структуры объектов (отношений "контейнеры ресурсов-ресурсы"), и для исключения обнаруженных противоречий формируют описание ошибок, допущенных при задании правил разграничения доступа субъектов к объектам на разных уровнях иерархии субъектов и объектов, а также производят коррекцию правил разграничения доступа соответствующей политики безопасности, исключая противоречивые правила или внося изменения в существующие правила и повторяя данную процедуру для всех правил до полного исключения противоречий.

Для настройки и контроля безопасности, осуществляемых в соответствии с

типовым шаблоном безопасности, выполняют перечисление конфигурационных параметров, заданных в выбранном шаблоне безопасности, затем итеративно по каждому из перечисленных параметров взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и, в случае осуществления настройки, настраивают данный конфигурационный параметр безопасности системы, либо, в случае контроля безопасности, фиксируют его наличие и текущее значение.

Настройку по политике безопасности осуществляют так же, как и настройку по типовым шаблонам безопасности, за исключением того, что уровни доступа, указанные в политике безопасности, настраивают в виде прямых прав доступа, снимая остальные права, предоставляемые для каждой настраиваемой пары "субъект-объект" другими конфигурационными параметрами безопасности и их значениями.

Настройку по зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы осуществляют так же, как и настройку по типовому шаблону безопасности.

Для анализа безопасности, осуществляемого в соответствии с политикой безопасности, анализа соответствия конфигурационных параметров безопасности зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы и анализа соблюдения правил эффективного администрирования информационной системы взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и фиксируют текущие состав и значения всех конфигурационных параметров безопасности.

Численный показатель эффективности администрирования системы определяют как среднее количество записей контроля доступа, т.е. масок прав доступа, меток доступа и целостности, установленных для пользователей системы. На изменение этого показателя оказывают влияние такие конфигурационные характеристики, изменяемые в ходе администрирования системы, как количество и вложенность субъектов (пользователей, групп) и иерархических объектов (файловой системы, реестра).

Расчет уровня доступа субъекта к объекту производят путем последовательного формирования множества доступных субъекту прав на основе прямых прав доступа объекта, заданных для конкретного субъекта, с учетом прав, распространяющихся по иерархиям субъектов и объектов, т.е. с учетом унаследованных, групповых и прямых разрешений и запретов; прав, соответствующих конфигурационным параметрам безопасности; прав, соответствующих значениям конфигурационных параметров безопасности; прав, назначенных на зависимые объекты в информационной системе; прав, получаемых из меток доступа и целостности.

Для решения технической задачи система, реализующая способ централизованных автоматизированных настройки, контроля и анализа безопасности информационных систем, включает блок управления конфигурационными параметрами безопасности и центральный блок контроля и анализа безопасности, в состав которых входят

модули управления конфигурационными параметрами безопасности, в совокупности образующие блок управления конфигурационными параметрами безопасности и дополнительно к функции сбора конфигурационных параметров безопасности выполняющие их настройку по заданным составу и значениям;

совокупность модулей, образующих центральный блок контроля и анализа безопасности, включая модуль сетевого взаимодействия и безопасности системы, помимо информационного и управляющего интерфейса центрального блока с блоком

управления конфигурационными параметрами безопасности, т.е. со всеми активными модулями управления конфигурационными параметрами безопасности, обеспечивающий контроль целостности программного состава системы, идентификацию модулей управления конфигурационными параметрами безопасности и защиту передаваемых данных;

модуль управления системой, помимо функции интеграции всех модулей центрального блока и предоставления пользовательского интерфейса оператору системы, обеспечивающий определение типа операционной среды информационной системы и подключение соответствующей модели контроля и управления доступом операционной среды, интерактивное взаимодействие с модулем редактирования требований безопасности, а также каталогизированное хранение зафиксированных состояний, шаблонов безопасности, политик безопасности и формируемых отчетов;

модуль описания модели контроля и управления доступом операционной среды, содержащей для соответствующего типа операционной среды правила расчета уровня доступа субъекта к объекту на основе состояния операционной среды;

модуль редактирования требований безопасности, предназначенный для генерации критериев безопасности системы путем задания условий безопасности системы, а также осуществляющий поиск, описание и коррекцию противоречий в указанных условиях, формирующий тем самым множество типовых шаблонов безопасности и политик безопасности, используемых при настройке, контроле и анализе безопасности информационной системы;

которые связаны посредством модуля управления системой с модулем процессора безопасности, помимо функций проверки безопасности осуществляющим расчет уровней доступа на множестве конфигурационных параметров безопасности, проверку выполнения условий безопасности системы, заданных в виде критериев из типовых шаблонов и политик безопасности, сопоставление зафиксированных состояний, оценку эффективности администрирования системы, выявление нарушений безопасности и их составов;

и с модулем формирования отчетов, помимо вывода результирующей информации в виде отчета дополнительно имеющим обратную связь через модуль управления и модуль сетевого взаимодействия и безопасности системы с модулями управления конфигурационными параметрами для осуществления настройки конфигурационных параметров безопасности и исправления обнаруженных нарушений безопасности.

Предлагаемые способ и система нацелены на настройку, контроль и анализ конфигурационных параметров безопасности по всем идентифицируемым сущностям операционной среды, их атрибутам безопасности, системным и программным опциям и установкам. В предлагаемых способе и системе предусмотрено создание произвольных типовых шаблонов и политик безопасности, на основе которых выполняется настройка, контроль и анализ безопасности информационных систем. Анализ безопасности задействует модель контроля и управления доступом, соответствующую типу операционной среды информационной системы, что позволяет осуществлять поддержку разнообразных систем путем адаптации модели без изменения конфигурации информационной системы и содержания предлагаемых способа и системы. Предлагаемые способ и система помимо предоставления результатов анализа безопасности в виде описания выявленных нарушений безопасности и набора инструкций, устраняющих обнаруженные нарушения, позволяют осуществлять настройку конфигурационных параметров безопасности, приводя их в соответствие с шаблонами и политиками безопасности или

зафиксированными (шаблонными) состояниями системы, и тем самым автоматически выявлять и устранять ошибки администрирования следующих типов: отклонения от типовых шаблонов безопасности; ошибки администрирования системных и пользовательских программ и ресурсов, допущенных при реализации политик безопасности; отклонения от зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы; проблемы управления системой, заключающихся в ее неэффективном администрировании. Примерами устраняемых нарушений безопасности являются изменение состава доступного пользователям программного обеспечения, первоначальных настроек пользовательской среды, исполняющихся сервисов и процессов; изменение пользовательского состав групп; несоблюдение базовых мер безопасности, представленных в системе в виде типовых шаблонов безопасности для различных операционных сред; отклонения от типовой программной конфигурации; ошибки реализации и отклонения от правил разграничения доступа политики безопасности; избыточность и сложность модификации заданных в системе конфигурационных параметров безопасности для системных и пользовательских информационных ресурсов; наличие неиспользуемых (выключенных) возможностей защиты программных средств контроля доступа; низкий уровень (недостаточность) защиты, определяемый конфигурационными параметрами программных средств контроля доступа. Поэтому предлагаемый способ и реализующая его система по многим параметрам превосходят возможности современных решений по настройке и анализу безопасности, которые осуществляют прямое сравнение множеств параметров информационной системы и при этом не используют никаких моделей и методов анализа.

Изобретение поясняется с помощью фиг.1-3. На фиг.1 представлена схема последовательности осуществления способа централизованных автоматизированных настройки, контроля и анализа безопасности информационных систем в части операций, проводимых по шаблону безопасности, политике безопасности или зафиксированному (шаблонному) состоянию системы. На фиг.2 приведена схема последовательности осуществления способа централизованных автоматизированных настройки, контроля и анализа безопасности информационных систем в части оценки эффективности администрирования системы. На фиг.3. представлена модульная схема системы, реализующей способ централизованных автоматизированных настройки, контроля и анализа безопасности информационных систем.

Основной задачей предлагаемых способа и системы является централизация и автоматизация управления безопасностью информационных систем в части настройки, контроля, анализа конфигурационных параметров безопасности и выявления нарушений безопасности, которые связаны с ошибками администрирования, допущенными в конфигурационных параметрах.

Основным источником нарушений безопасности информационных систем является огромное количество уязвимостей, которыми пользуются нарушители для осуществления несанкционированного доступа или организации отказа в обслуживании. Уязвимости возникают вследствие ошибок, допущенных в ходе проектирования, программирования и администрирования информационных систем. Наибольшее распространение получили ошибки программирования, которые производители регулярно исправляют с помощью обновлений кода (так называемых "патчей", "пакетов обновлений"). В то же время статистические данные, полученные такими авторитетными организациями, как CERT и Secunia, свидетельствуют о том, что более 20% видов уязвимостей имеют причиной своего возникновения ошибочные

действия администраторов и пользователей. Суть администрирования в контексте информационной безопасности составляет настройка механизмов защиты информационной системы, т.е. задание параметров, влияющих на конфиденциальность, целостность и доступность системных и пользовательских информационных ресурсов, функционирование средств защиты, приложений и информационных систем в целом. Множество таких параметров, настраиваемых в процессе администрирования, будем называть конфигурационными параметрами безопасности. К таким параметрам относятся, например, привилегии пользователей, членство пользователей в группах, права доступа к файлам и каталогам. Ошибки, допущенные в ходе настройки безопасности, являются причинами уязвимостей конфигурационных параметров безопасности, и, как следствие, приводят к нарушениям безопасности информационных систем.

Проявление уязвимостей конфигурационных параметров безопасности обусловлено несоблюдением мер безопасности, рекомендованных экспертами по защите информации, разработчиками операционных сред и производителями программного обеспечения; противоречивостью и ошибками реализации правил разграничения доступа, заданных в политиках безопасности; отступлением от принципа эффективного администрирования информационных систем; невыполнением типовой программной конфигурации.

Уязвимости конфигурационных параметров безопасности невозможно устранить с помощью обновлений программных модулей, исправляющих ошибки кодирования, или применения дополнительных средств защиты, усиливающих возможности штатных механизмов контроля и управления доступом. Для обеспечения безопасности обслуживаемой информационной системы и выполнения корпоративной политики безопасности квалифицированный администратор должен постоянно анализировать сведения о нарушениях безопасности и следовать актуальным рекомендациям по поддержанию защиты информации, что составляет нетривиальную задачу, так как требует оперативного выявления нарушений безопасности, локализации и перезадания параметров, вызвавших их появление. Для этого необходимо обладать глубокими знаниями об особенностях работы обслуживаемых информационных систем и программных средств защиты, постоянно анализировать значения огромного множества конфигурационных параметров безопасности. Например, в операционной среде Windows насчитывается более 30 типов объектов защиты прикладного уровня (учетные записи пользователей, объекты файловой системы и реестра, сервисы, принтеры и т.д.) и уровня ядра (процессы, потоки, объекты синхронизации и т.д.). Для каждого объекта защиты поддерживается маска прав размером 32 бита доступа. В иерархии файловой системы и реестра доступ к объекту определяется не только прямыми правами, заданными к объекту, но и унаследованными от объектов-контейнеров, расположенных выше по иерархии. Кроме того, на возможность доступа влияют привилегии, назначаемые пользователям и группам, и параметры локальной и групповой политик безопасности. Таким образом, количество возможных значащих комбинаций конфигурационных параметров безопасности, требующих от администратора постоянного мониторинга и вмешательства, исчисляется многими миллионами. Таким образом, для администрирования информационных систем необходим соответствующий инструментарий, который позволял бы управлять внушительным объемом конфигурационных параметров безопасности.

Предлагаемый способ осуществляется путем выполнения следующих действий

(фиг.1-2).

Первоначально задают требования безопасности, на соответствие которым выполняется настройка, контроль или анализ безопасности информационной системы. При этом задаваемые требования безопасности составляют типовой шаблон безопасности, политику безопасности или зафиксированное (шаблонное) состояние системы.

При создании типового шаблона безопасности основываются на рекомендациях по безопасной базовой настройке системных информационных ресурсов соответствующей операционной среды (например, для операционных сред Windows: Murugiah Souppaya, Karen Kent, Paul M. Johnson "Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist" csrc.nist.gov/itsec/SP800-68-20051102.pdf$; "NSA Windows XP Security Guide Addendum"; www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/winxp/NSA_Windows_XP_Security_Guide_Addendum.pdf; "Microsoft Windows 2000 Network Architecture Guide"; www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_net_arch_guide.pdf; "Windows Server 2003 Security Guide"; www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2003/MSCG - 001R-2003.pdf; "Windows 2000 Security Hardening Guide" www.microsoft.com/downloads/details.aspx?FamilylD=15E83186-A2C8-4C8F-A9DO-A0201F639A56&DisplayLang=en; "Windows XP Security Hardening Guide" www.microsoft.com/Downloads/details.aspx?familyid=2D3E25BC-F434-4CC6-A5A7-09A8A229F118&displaylang=en; "Windows 2003 Security Hardening Guide"; www.microsoft.com/technet/security/prodtech/windowsserver2003/w200 3hg/sgch00.mspx; Дистрибутив Windows 2000/XP/2003, каталог %systemdir%\security\templates; "Операционная система Microsoft Windows Server 2003. Руководство по безопасной настройке и контролю сертифицированной версии", http://altx-soft.ru/rbn_Server_2003_(Ent-St).pdf; "Операционная система Microsoft Windows XP Professional. Руководство по безопасной настройке и контролю сертифицированной версии", www.altx.ru/po_rukovodstvo.pdf). При этом каждая рекомендация, составляющая типовой шаблон безопасности, образует критерий безопасности системы, представляемый в виде кортежей "Состав конфигурационных параметров безопасности" или "Значение конфигурационного параметра безопасности", описывающих условия безопасности системы в виде множества конфигурационных параметров или их значений, соответственно. В зависимости от того, какие задачи решает узел сети (рабочая станция или сервер) и какая операционная среда на нем развернута, формулируются определенные наборы рекомендаций по безопасной базовой настройке информационных ресурсов. В состав системы включены типовые шаблоны безопасности для типовых назначений рабочих станций и серверов.

Политики безопасности составляют на основе корпоративных требований контроля и управления доступом, выдвигаемых к информационной системе, с учетом их выполнения в соответствующей операционной среде (Windows, UNIX и т.п.). При создании политики безопасности основываются на требованиях безопасности, составляющих правила разграничения доступа субъектов к объектам. При этом из каждого правила разграничения доступа, составляющего политику безопасности, формируют критерий безопасности системы, представляемый в виде кортежа "Субъект-объект-уровень доступа", описывающего условие, при соблюдении которого система является безопасной. Политики безопасности расширяют область действия типовых шаблонов безопасности за счет учета пользовательских информационных ресурсов помимо системных.

В правилах разграничения доступа созданной политики безопасности производят поиск противоречий в указанных уровнях доступа субъектов к объектам с учетом иерархической структуры субъектов (отношений "группы пользователей-пользователи") и иерархической структуры объектов (отношений "контейнеры ресурсов-ресурсы") и, в случае обнаружения противоречий, формируют описание ошибок, допущенных при задании правил разграничения доступа субъектов к объектам на разных уровнях иерархии субъектов и объектов, а также производят коррекцию правил разграничения доступа соответствующей политики безопасности, исключая противоречивые правила или внося изменения в существующие правила и повторяя данную процедуру для всех правил до полного исключения противоречий.

При задании требований безопасности в виде зафиксированного (шаблонного) состояния системы взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и фиксируют состав текущих конфигурационных параметров безопасности и их действующие значения, формируя зафиксированное состояние безопасности информационной системы. Повторяют это действие необходимое количество раз для необходимого количества узлов информационной системы, формируя множество зафиксированных состояний безопасности по каждому узлу. При этом в качестве состояния информационной системы рассматривают все множество конфигурационных параметров безопасности, а именно субъекты, объекты и их атрибуты безопасности, состав которых определяется типом операционной среды информационной системы. В общем случае состояние безопасности составляют такие конфигурационные параметры безопасности, как пользователи и группы пользователей; элементы файловой системы (диски, каталоги, файлы, ссылки), элементы реестра (разделы, ключи, параметры, ссылки); объекты ядра (задачи, процессы, потоки, драйверы, объекты синхронизации и т.д.); ресурсы общего доступа (каталоги, принтеры); программные сервисы; COM/DCOM-объекты; объекты службы каталога; локальные и глобальные настройки системной политики безопасности; опции и настройки безопасности пользовательского и специального программного обеспечения; конфигурационные параметры сетевых служб; атрибуты безопасности субъектов и объектов (идентификаторы защиты, привилегии пользователей и групп пользователей, информация о владельцах объектов, списки прав доступа, метки доступа и целостности, иерархическое распределение субъектов, объектов, прав доступа, меток доступа и целостности).

После этого выполняют выбор эталонной конфигурации безопасности, на которой будет в дальнейшем производиться настройка, контроль или анализ.

В случае если требования безопасности сформулированы виде типового шаблона, политики безопасности или зафиксированного (шаблонного) состояния, то из множества созданных типовых шаблонов и политик безопасности выбирают шаблон или политику, по составляющим критериям которых должна быть выполнена настройка, или на соответствие которым должны контролироваться конфигурационные параметры безопасности, или должна быть проанализирована безопасность системы.

При выполнении настройки конфигурационных параметров безопасности взаимодействуют с программными средствами контроля и управления доступом операционной среды информационной системы, выполняют установку значений конфигурационных параметров безопасности в соответствии с выбранным типовым шаблоном или политикой безопасности и составляют отчет о настройке безопасности,

содержащий сведения об изменяемых конфигурационных параметрах безопасности и о результатах установки их значений. При этом для настройки, осуществляемой в соответствии с типовым шаблоном или политикой безопасности, выполняют перечисление конфигурационных параметров, заданных в выбранном шаблоне или политике безопасности, затем итеративно по каждому из перечисленных параметров взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и настраивают данный конфигурационный параметр безопасности системы. При этом уровни доступа, указанные в политике безопасности, настраивают в виде прямых прав доступа, снимая остальные права, предоставляемые для каждой настраиваемой пары "субъект-объект" другими конфигурационными параметрами безопасности и их значениями. Настройку по зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы осуществляют так же, как и настройку по типовому шаблону безопасности.

При выполнении контроля или анализа конфигурационных параметров безопасности либо взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и фиксируют состав текущих конфигурационных параметров безопасности и их действующие значения, формируя зафиксированное состояние безопасности информационной системы; либо из множества ранее зафиксированных состояний безопасности информационной системы выбирают состояние, на котором должны быть проконтролированы конфигурационные параметры безопасности или должна быть проанализирована безопасность системы.

При этом для контроля безопасности, осуществляемого в соответствии с типовым шаблоном безопасности, выполняют перечисление конфигурационных параметров, заданных в выбранном шаблоне безопасности, затем итеративно по каждому из перечисленных параметров взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и фиксируют его наличие и текущее значение.

Для анализа безопасности, осуществляемого в соответствии с политикой безопасности, анализа соответствия конфигурационных параметров безопасности зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы и анализа соблюдения правил эффективного администрирования информационной системы взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и фиксируют текущие состав и значения всех конфигурационных параметров безопасности.

Далее на текущем или выбранном зафиксированном состоянии безопасности информационной системы контролируют и анализируют следующим образом выполнение требований безопасности: типовых шаблонов безопасности, построенных на основе рекомендаций по безопасной настройке операционной среды информационной системы; правил разграничения доступа политик безопасности; зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы; правил эффективного администрирования систем.

В случае контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Состав конфигурационных параметров безопасности", если выбрано текущее состояние, то взаимодействуют со штатными

программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав зафиксированных конфигурационных параметров безопасности, затем сравнивают множества зафиксированных конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, выявляют их различия и по результатам сравнения составляют отчет о контроле безопасности, содержащий описание выявленных отклонений от типового шаблона безопасности по составу конфигурационных параметров безопасности и инструкции по изменению состава конфигурационных параметров безопасности для устранения выявленных отклонений.

В случае контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Значение конфигурационного параметра безопасности", если выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности и затем сравнивают множества зафиксированных конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, сравнивают для подтвержденных конфигурационных параметров, указанных в выбранном типовом шаблоне безопасности и зафиксированных в системе, множества значений конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, выявляют их различия и составляют отчет о контроле безопасности, содержащий описание выявленных отклонений от типового шаблона безопасности по составу и значениям конфигурационных параметров безопасности и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных отклонений.

В случае анализа безопасности системы выполняют проверку соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в политике безопасности в виде кортежей "Субъект-объект-уровень доступа". При этом если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности и затем сравнивают множества зафиксированных конфигурационных параметров безопасности с указанными в выбранной политике безопасности в части подмножеств субъектов и объектов, рассчитывают для всех подтвержденных пар "субъект-объект", указанных в выбранной политике безопасности и зафиксированных в системе, действующие уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех текущих зафиксированных конфигурационных параметров безопасности и их значений и затем сравнивают значения рассчитанных действующих уровней доступа с указанными в выбранной политике безопасности, выявляя их различия, фиксируя состав и значения конфигурационных параметров, послуживших факторами влияния на отклонения уровней доступа, и составляя отчет об анализе безопасности,

содержащий описание выявленных ошибок администрирования системных и пользовательских программ и ресурсов, допущенных при реализации политики безопасности, по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и инструкции по изменению состава конфигурационных параметров безопасности и их значений для устранения выявленных нарушений и факторов влияния на уровни доступа.

При этом расчет уровня доступа субъекта к объекту производят путем последовательного формирования множества доступных субъекту прав на основе прямых прав доступа объекта, заданных для конкретного субъекта, с учетом прав, распространяющихся по иерархиям субъектов и объектов, т.е. с учетом унаследованных, групповых и прямых разрешений и запретов; прав, соответствующих конфигурационным параметрам безопасности; прав, соответствующих значениям конфигурационных параметров безопасности; прав, назначенных на зависимые объекты в информационной системе; прав, получаемых из меток доступа и целостности.

В случае анализа соответствия конфигурационных параметров безопасности зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы, если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, затем из множества ранее зафиксированных состояний безопасности информационной системы выбирают еще одно состояние, которое определяется как зафиксированное (шаблонное) безопасное состояние, после чего сравнивают текущие конфигурационные параметры безопасности с указанными в зафиксированном (шаблонном) безопасном состоянии по составу и значениям, рассчитывают для всех подтвержденных пар "субъект-объект", указанных в выбранном зафиксированном (шаблонном) безопасном состоянии и зафиксированных в системе, действующие уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех текущих зафиксированных конфигурационных параметров безопасности и их значений, рассчитывают для тех же пар "субъект-объект" требуемые уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех конфигурационных параметров безопасности и их значений, указанных в зафиксированном (шаблонном) безопасном состоянии, сравнивают рассчитанные действующие и требуемые уровни доступа и составляют отчет об анализе безопасности, содержащий описание выявленных отклонений от зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных отклонений и факторов влияния на уровни доступа.

В случае анализа соблюдения правил эффективного администрирования информационной системы, если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления

доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, оценивают по ним эффективность администрирования системы и объявляют ее эталонной, и после чего контролируют возникновение проблем управления системой, заключающихся в неэффективном администрировании системы, удаленно взаимодействуя со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируя состав и значения текущих конфигурационных параметров безопасности, оценивая по ним текущую эффективность администрирования системы, выполняя сравнение эталонного значения эффективности администрирования системы с текущим, определяя численные характеристики, снижающие эффективность администрирования системы, и составляя отчет об анализе безопасности, содержащий описание проблем управления системой, заключающихся в неэффективном администрировании системы, график изменения эффективности администрирования системы с течением времени, перечень численных характеристик, снижающих эффективность, и рекомендации по повышению эффективности администрирования системы.

При этом численный показатель эффективности администрирования системы определяют как среднее количество записей контроля доступа, т.е. прав доступа, меток доступа и целостности, установленных для пользователей системы. На изменение этого показателя оказывают влияние такие конфигурационные характеристики, изменяемые в ходе администрирования системы, как количество и вложенность субъектов (пользователей, групп) и иерархических объектов (файловой системы, реестра).

С целью устранения нарушений безопасности, выявленных при контроле и анализе по требованиям безопасности, сформулированным в типовых шаблонах, политиках безопасности и зафиксированных (шаблонных) состояниях, производят настройку конфигурационных параметров безопасности в соответствии с инструкциями, сформированными в отчетах о контроле безопасности или в отчетах об анализе безопасности, и составляют отчет о настройке безопасности (3), содержащий сведения об изменяемых конфигурационных параметрах безопасности и о результатах установки их значений.

Периодически повторяют в необходимой последовательности вышеуказанные действия по настройке, фиксации, контролю и анализу конфигурационных параметров безопасности и составляют множество отчетов о контроле, анализе и настройке безопасности, тем самым непрерывно обеспечивая безопасность информационной системы.

Данные, полученные в результате применения указанного способа, позволяют устранять ошибки, допущенные в конфигурационных параметрах безопасности в текущем состоянии системы и которые могут возникнуть в ходе ее эксплуатации.

Для автоматизации предложенного способа применяют систему (фиг.3), которая включает блок управления конфигурационными параметрами безопасности 4 и центральный блок контроля и анализа безопасности 5, в состав которых входят модули управления конфигурационными параметрами безопасности 6, в совокупности образующие блок управления конфигурационными параметрами безопасности и совокупность модулей, образующих центральный блок контроля и анализа безопасности 5, включая модуль сетевого взаимодействия и безопасности системы 7,

связывающий центральный блок 5 со всеми активными модулями управления конфигурационными параметрами безопасности; модуль управления системой 8, связывающий все модули центрального блока 5 и обеспечивающий подключение модуля описания модели контроля и управления доступом операционной среды 9, взаимодействие с модулем редактирования требований безопасности 10; модуль описания модели контроля и управления доступом операционной среды 9 и модуль редактирования требований безопасности 10, которые связаны посредством модуля управления системой 8 с модулем процессора безопасности 11, а также с модулем формирования отчетов 12, имеющим обратную связь через модуль управления и модуль сетевого взаимодействия и безопасности системы 7 с модулями управления конфигурационными параметрами 6.

Способ централизованных автоматизированных настройки, контроля и анализа безопасности информационных систем реализуют в предлагаемой системе следующим образом.

Модули управления конфигурационными параметрами 6 безопасности помимо сбора конфигурационных параметров безопасности выполняют их настройку по заданным составу и значениям. Количество используемых в системе модулей управления конфигурационными параметрами безопасности 6 определяется количеством анализируемых и настраиваемых узлов информационной системы (рабочих станций и серверов). Реализация модулей 6 определяется типом операционной среды информационной системы. В общем случае модули 6 взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды 9 информационной системы и либо фиксируют состав текущих конфигурационных параметров безопасности и их действующие значения, формируя зафиксированное состояние безопасности информационной системы, либо определяют новое состояние безопасности информационной системы, при этом управляя такими конфигурационными параметрами безопасности, как пользователи и группы пользователей; элементы файловой системы (диски, каталоги, файлы, ссылки), элементы реестра (разделы, ключи, параметры, ссылки); объекты ядра (задачи, процессы, потоки, драйверы, объекты синхронизации и т.д.); ресурсы общего доступа (каталоги, принтеры); программные сервисы; COM/DCOM-объекты; объекты службы каталога; локальные и глобальные настройки системной политики безопасности; опции и настройки безопасности пользовательского и специального программного обеспечения; конфигурационные параметры сетевых служб; атрибуты безопасности субъектов и объектов (идентификаторы защиты, привилегии пользователей и групп пользователей, информация о владельцах объектов, списки прав доступа, метки доступа и целостности, иерархическое распределение субъектов, объектов, прав доступа, меток доступа и целостности).

Результатом работы модулей управления конфигурационными параметрами безопасности 6 является либо множество зафиксированных состояний информационной системы, либо модифицированное при настройке множество конфигурационных параметров безопасности.

Модули управления конфигурационными параметрами 6 безопасности образуют блок управления конфигурационными параметрами безопасности 4, остальные модули формируют ее центральный блок 5.

Модуль сетевого взаимодействия и безопасности системы 7 обеспечивает информационный и управляющий интерфейс центрального блока 5 с блоком управления конфигурационными параметрами безопасности 4, т.е. со всеми

активными модулями управления конфигурационными параметрами безопасности, а также осуществляет контроль целостности программного состава системы, идентификацию модулей управления конфигурационными параметрами безопасности и защиту передаваемых данных.

Модуль управления системой 8 связывает все модули центрального блока 5, предоставляет пользовательский интерфейс оператору системы, а также обеспечивает определение типа операционной среды информационной системы, подключение модуля описания модели контроля и управления доступом операционной среды 9, интерактивное взаимодействие с модулем редактирования требований безопасности 10, каталогизированное хранение зафиксированных состояний, шаблонов безопасности, политик безопасности и формируемых отчетов.

Модуль описания модели контроля и управления доступом операционной среды 9 содержит правила расчета уровня доступа субъекта к объекту на основе зафиксированного состояния соответствующей операционной среды, а именно формирования множества прямых прав доступа объекта, заданных для конкретного субъекта, с учетом прав, распространяющихся по иерархиям субъектов и объектов, т.е. с учетом унаследованных, групповых и прямых разрешений и запретов; прав, соответствующих конфигурационным параметрам безопасности; прав, соответствующих значениям конфигурационных параметров безопасности; прав, назначенных на зависимые объекты в информационной системе; прав, получаемых из меток доступа и целостности. Для каждого типа операционной среды в системе определяют и подключают соответствующую модель контроля и управления доступом операционной среды.

Модуль редактирования требований безопасности 10 осуществляет генерацию критериев безопасности системы путем задания условий безопасности системы. Модуль редактирования требований безопасности 10 позволяет создавать критерии безопасности системы, представляемые в виде кортежей "Состав конфигурационных параметров безопасности", "Значение конфигурационного параметра безопасности" или "Субъект-объект-уровень доступа", описывающих, соответственно, множества конфигурационных параметров, их значения или отношения множеств субъектов, объектов и заданных для них уровней доступа, при соблюдении которых информационная система является безопасной. При составлении политики безопасности модуль редактирования требований безопасности 10 осуществляет также поиск противоречий в указанных уровнях доступа субъектов к объектам, определяя во множестве кортежей "Субъект-объект-уровень доступа" наличие ограничений, заданных для одной пары "субъект-объект", но с разными уровнями доступа, с учетом иерархической структуры субъектов (отношений "группы пользователей - пользователи") и иерархической структуры объектов (отношений "контейнеры ресурсов - ресурсы"), и для исключения обнаруженных противоречий формирует описание ошибок, допущенных при задании правил разграничения доступа субъектов к объектам на разных уровнях иерархии субъектов и объектов, а также позволяет произвести коррекцию правил разграничения доступа соответствующей политики безопасности с целью исключения противоречивых правил или внесения изменений в существующие правила. Тем самым результатом работы модуля редактирования требований безопасности 10 является множество типовых шаблонов безопасности и политик безопасности, используемых при настройке, контроле и анализе безопасности информационной системы.

Модуль описания модели контроля и управления доступом операционной среды 9 и

модуль редактирования требований безопасности 10 связаны посредством модуля управления системой 8 с модулем процессора безопасности 11, который выполняет расчет уровней доступа на множестве конфигурационных параметров безопасности, проверку выполнения условий безопасности системы, заданных в виде критериев из типовых шаблонов и политик безопасности, сопоставление зафиксированных состояний, оценку эффективности администрирования системы, выявление нарушений безопасности и их составов.

При настройке, осуществляемой в соответствии с типовым шаблоном или политикой безопасности, модуль процессора безопасности 11 выполняет перечисление конфигурационных параметров, заданных в выбранном шаблоне или политике безопасности, затем итеративно по каждому из перечисленных параметров взаимодействуют с соответствующим активным модулем управления конфигурационными параметрами безопасности с целью настройки данного конфигурационного параметра безопасности системы. При этом уровни доступа, указанные в политике безопасности, настраивают в виде прямых прав доступа, снимая остальные права, предоставляемые для каждой настраиваемой пары "субъект-объект" другими конфигурационными параметрами безопасности и их значениями. Настройку по зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы осуществляют так же, как и настройку по типовому шаблону безопасности.

При выполнении контроля или анализа конфигурационных параметров безопасности модуль процессора безопасности 11 либо взаимодействует с соответствующим модулем управления конфигурационными параметрами безопасности 6 и получает от него состав текущих конфигурационных параметров безопасности и их действующие значения, либо получает выбранное оператором ранее зафиксированное состояние безопасности информационной системы, на котором должны быть проконтролированы конфигурационные параметры безопасности или должна быть проанализирована безопасность системы.

При контроле безопасности, осуществляемом в соответствии с типовым шаблоном безопасности, модуль процессора безопасности 11 выполняет перечисление конфигурационных параметров, заданных в выбранном шаблоне безопасности, что позволяет соответствующему модулю управления конфигурационными параметрами безопасности 6 итеративно по каждому из перечисленных параметров зафиксировать его наличие и текущее значение.

При анализе безопасности, осуществляемом в соответствии с политикой безопасности, анализе соответствия конфигурационных параметров безопасности зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы и анализе соблюдения правил эффективного администрирования информационной системы модуль процессора безопасности 11 инициирует фиксацию текущих состава и значений всех конфигурационных параметров безопасности.

Далее на текущем или выбранном зафиксированном состоянии безопасности информационной системы модуль процессора безопасности 11 контролирует и анализирует следующим образом выполнение требований безопасности: типовых шаблонов безопасности, построенных на основе рекомендаций по безопасной настройке операционной среды информационной системы; правил разграничения доступа политик безопасности; зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы; правил эффективного

администрирования систем.

В случае контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Состав конфигурационных параметров безопасности", если выбрано текущее состояние, то модуль процессора безопасности инициирует фиксацию состава текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то модуль процессора безопасности 11 извлекает из него состав зафиксированных конфигурационных параметров безопасности и затем сравнивает множества зафиксированных конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, выявляет их различия по составу конфигурационных параметров безопасности и необходимые изменения состава конфигурационных параметров безопасности, необходимые для устранения выявленных отклонений.

В случае контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Значение конфигурационного параметра безопасности", если выбрано текущее состояние, то модуль процессора безопасности инициирует фиксацию состава и значений текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то модуль процессора безопасности 11 извлекает из него состав и значения зафиксированных конфигурационных параметров безопасности и затем сравнивает множества зафиксированных конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, сравнивает для подтвержденных конфигурационных параметров, указанных в выбранном типовом шаблоне безопасности и зафиксированных в системе, множества значений конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, выявляет их различия по составу и значениям конфигурационных параметров безопасности и изменения состава и значений конфигурационных параметров безопасности, необходимые для устранения выявленных отклонений.

В случае анализа безопасности системы модуль процессора безопасности 11 выполняет проверку соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в политике безопасности в виде кортежей "Субъект-объект-уровень доступа". При этом, если для анализа выбрано текущее состояние, то модуль процессора безопасности 11 инициирует фиксацию состава и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то модуль процессора безопасности 11 извлекает из него состав и значения зафиксированных конфигурационных параметров безопасности и затем сравнивает множества зафиксированных конфигурационных параметров безопасности с указанными в выбранной политике безопасности в части подмножеств субъектов и объектов, рассчитывает для всех подтвержденных пар "субъект-объект", указанных в выбранной политике безопасности и зафиксированных в системе, действующие уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех текущих зафиксированных конфигурационных параметров безопасности и их значений и затем сравнивает значения рассчитанных действующих уровней доступа с указанными в выбранной политике безопасности, выявляя их различия, фиксируя состав и значения конфигурационных параметров, послуживших факторами влияния на отклонения уровней доступа, перечень конфигурационных параметров безопасности и их

значений, составляющих выявленные нарушения, и изменения состава конфигурационных параметров безопасности и их значений, необходимых для устранения выявленных нарушений и факторов влияния на уровни доступа.

При этом расчет уровня доступа субъекта к объекту модуль процессора безопасности 11 производит с использованием правил соответствующей модели контроля и управлении доступом путем последовательного формирования множества прав доступа на основе прямых прав доступа объекта, заданных для конкретного субъекта, с учетом прав, распространяющихся по иерархиям субъектов и объектов, т.е. с учетом унаследованных, групповых и прямых разрешений и запретов; прав, соответствующих конфигурационным параметрам безопасности; прав, соответствующих значениям конфигурационных параметров безопасности; прав, назначенных на зависимые объекты в информационной системе; прав, получаемых из меток доступа и целостности.

В случае анализа соответствия конфигурационных параметров безопасности зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы, если для анализа выбрано текущее состояние, то модуль процессора безопасности 11 инициирует фиксацию состава и значений текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то модуль процессора безопасности 11 извлекает из него состав и значения зафиксированных конфигурационных параметров безопасности, затем сравнивает текущие конфигурационные параметры безопасности с указанными в зафиксированном (шаблонном) безопасном состоянии по составу и значениям, рассчитывает для всех подтвержденных пар "субъект-объект", указанных в выбранном зафиксированном (шаблонном) безопасном состоянии и зафиксированных в системе, действующие уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех текущих зафиксированных конфигурационных параметров безопасности и их значений, рассчитывает для тех же пар "субъект-объект" требуемые уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех конфигурационных параметров безопасности и их значений, указанных в зафиксированном (шаблонном) безопасном состоянии, сравнивает рассчитанные действующие и требуемые уровни доступа и фиксирует отклонения от зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и изменения состава и значений конфигурационных параметров безопасности, необходимые для устранения выявленных отклонений и факторов влияния на уровни доступа.

В случае анализа соблюдения правил эффективного администрирования информационной системы, если для анализа выбрано текущее состояние, то модуль процессора безопасности 11 инициирует фиксацию состава и значений текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то модуль процессора безопасности 11 извлекает из него состав и значения зафиксированных конфигурационных параметров безопасности, оценивает по ним эталонную эффективность администрирования системы, после чего контролирует возникновение проблем управления системой, заключающихся в неэффективном администрировании системы, инициируя фиксацию состава и значений текущих конфигурационных параметров безопасности, оценивая по ним текущую

эффективность администрирования системы, выполняя сравнение эталонного значения эффективности администрирования системы с текущим, определяя снижение эффективности администрирования системы и фиксируя проблемы управления системой, заключающиеся в неэффективном администрировании системы, график изменения эффективности администрирования системы с течением времени, перечень численных характеристик, снижающих эффективность, и изменения в принципах администрирования системы, необходимые для повышения эффективности. При этом модуль процессора безопасности 11 определяет численный показатель эффективности администрирования системы как среднее количество записей контроля доступа, т.е. прав доступа, меток доступа и целостности, установленных для пользователей системы. Модуль процессора безопасности 11 учитывает влияние на этот показатель таких конфигурационных характеристик, изменяемых в ходе администрирования системы, как количество и вложенность субъектов (пользователей, групп) и иерархических объектов (файловой системы, реестра).

Модуль процессора безопасности 11 связан с модулем формирования отчетов 12, который на основе результатов работы модуль процессора безопасности 11 генерирует отчеты, являющиеся результатами работы системы.

При выполнении настройки конфигурационных параметров безопасности модуль формирования отчетов 12 составляет отчет о настройке безопасности, содержащий сведения об изменяемых конфигурационных параметрах безопасности и о результатах установки их значений

В случае контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Состав конфигурационных параметров безопасности", модуль формирования отчетов 12 составляет отчет о контроле безопасности, содержащий описание выявленных отклонений от типового шаблона безопасности по составу конфигурационных параметров безопасности и инструкции по изменению состава конфигурационных параметров безопасности для устранения выявленных отклонений.

В случае контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Значение конфигурационного параметра безопасности", модуль формирования отчетов 12 составляет отчет о контроле безопасности, содержащий описание выявленных отклонений от типового шаблона безопасности по составу и значениям конфигурационных параметров безопасности и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных отклонений.

В случае анализа безопасности системы выполняют проверку соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в политике безопасности в виде кортежей "Субъект-объект-уровень доступа", модуль формирования отчетов 12 составляет отчет об анализе безопасности, содержащий описание выявленных ошибок администрирования системных и пользовательских программ и ресурсов, допущенных при реализации политики безопасности, по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и инструкции по изменению состава конфигурационных параметров безопасности и их значений для устранения выявленных нарушений и

факторов влияния на уровни доступа.

В случае анализа соответствия конфигурационных параметров безопасности зафиксированному (шаблонному) безопасному состоянию операционной среды информационной системы модуль формирования отчетов 12 составляет отчет об анализе безопасности, содержащий описание выявленных отклонений от зафиксированных (шаблонных) безопасных состояний операционной среды информационной системы по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных отклонений и факторов влияния на уровни доступа.

В случае анализа соблюдения правил эффективного администрирования информационной системы модуль формирования отчетов 12 составляет отчет об анализе безопасности, содержащий описание проблем управления системой, заключающихся в неэффективном администрировании системы, график изменения эффективности администрирования системы с течением времени, перечень численных характеристик, снижающих эффективность, и рекомендации по повышению эффективности администрирования системы.

Модуль формирования отчетов 12 дополнительно имеет обратную связь через модуль управления 8 и модуль сетевого взаимодействия и безопасности системы 7 с соответствующими модулями управления конфигурационными параметрами 6 для осуществления настройки конфигурационных параметров безопасности с целью исправления обнаруженных нарушений безопасности в соответствии с инструкциями, приведенными в отчетах, составленных модулем формирования отчетов 12.

Тем самым система обеспечивает повышение уровня безопасности информации путем автоматизации и централизации анализа и устранения уязвимостей конфигурационных параметров безопасности.

Таким образом, предлагаемые способ и система реализуют централизованное удаленное управление безопасностью информационных систем путем настройки значений конфигурационных параметров информационных систем, фиксацию и автоматический анализ заданной системной конфигурации, выявление нарушений безопасности, вызванных допущенными в ходе администрирования ошибками.

Формула изобретения

1. Способ централизованного автоматизированного управления параметрами безопасности операционных систем семейства Windows, включающий сбор информации, настройку системы безопасности по шаблонам, анализ конфигурационных параметров, создание отчета о состоянии безопасности, отличающийся тем, что создают типовой шаблон безопасности на основании рекомендаций по безопасной базовой настройке операционной среды информационных систем;

создают политику безопасности на основании требований безопасности, составляющих правила разграничения доступа субъектов к объектам;

при этом из каждой рекомендации, составляющей типовой шаблон безопасности, формируют критерий безопасности системы, представляемый в виде кортежей "Состав конфигурационных параметров безопасности" или "Значение конфигурационного параметра безопасности", описывающих условия, при соблюдении которых система

является безопасной;

при этом из каждого правила разграничения доступа, составляющего политику безопасности, формируют критерий безопасности системы, представляемый в виде кортежа "Субъект-объект-уровень доступа", описывающего условие, при соблюдении которого система является безопасной;

в правилах разграничения доступа созданной политики безопасности производят поиск противоречий в указанных уровнях доступа субъектов к объектам с учетом иерархической структуры субъектов и иерархической структуры объектов и, в случае обнаружения противоречий, формируют описание ошибок, допущенных при задании правил разграничения доступа субъектов к объектам на разных уровнях иерархии субъектов и объектов, а также производят коррекцию правил разграничения доступа соответствующей политики безопасности, исключая противоречивые правила или внося изменения в существующие правила и повторяя данную процедуру для всех правил до полного исключения противоречий;

из множества созданных типовых шаблонов и политик безопасности выбирают шаблон или политику, по составляющим критериям которых должна быть выполнена настройка, или на соответствие которым должны контролироваться конфигурационные параметры безопасности, или должна быть проанализирована безопасность системы;

при выполнении настройки конфигурационных параметров безопасности взаимодействуют с программными средствами контроля и управления доступом операционной среды информационной системы, выполняют установку значений конфигурационных параметров безопасности в соответствии с выбранным типовым шаблоном или политикой безопасности и составляют отчет о настройке безопасности, содержащий сведения об изменяемых конфигурационных параметрах безопасности и о результатах установки их значений;

при выполнении контроля или анализа конфигурационных параметров безопасности взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и фиксируют состав текущих конфигурационных параметров безопасности и их действующие значения, формируя зафиксированное состояние безопасности информационной системы;

из множества зафиксированных состояний безопасности информационной системы выбирают состояние, на котором должны быть проконтролированы конфигурационные параметры безопасности или должна быть проанализирована безопасность системы;

на текущем или выбранном зафиксированном состоянии безопасности информационной системы контролируют и анализируют выполнение требований безопасности: типовых шаблонов безопасности, построенных на основе рекомендаций по безопасной настройке операционной среды информационной системы; правил разграничения доступа политик безопасности; зафиксированных безопасных состояний операционной среды информационной системы; правил эффективного администрирования систем;

при этом в случае осуществления контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Состав конфигурационных параметров безопасности", если выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления

доступом операционной среды информационной системы, фиксируют состав текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав зафиксированных конфигурационных параметров безопасности, и затем сравнивают множества зафиксированных конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, выявляют их различия и по результатам сравнения составляют отчет о контроле безопасности, содержащий описание выявленных отклонений от типового шаблона безопасности по составу конфигурационных параметров безопасности и инструкции по изменению состава конфигурационных параметров безопасности для устранения выявленных отклонений;

при этом в случае осуществления контроля соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в типовом шаблоне безопасности в виде кортежей "Значение конфигурационного параметра безопасности", если выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, и затем сравнивают множества зафиксированных конфигурационных параметров безопасности с указанными в выбранном шаблоне безопасности, сравнивают для подтвержденных конфигурационных параметров, указанных в выбранном типовом шаблоне безопасности и зафиксированных в системе, множества значений конфигурационных параметров безопасности с указанными в выбранном шаблоне или в политике безопасности, выявляют их различия и составляют отчет о контроле безопасности, содержащий описание выявленных отклонений от типового шаблона безопасности по составу и значениям конфигурационных параметров безопасности и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных отклонений;

при этом в случае осуществления анализа безопасности системы выполняют проверку соответствия конфигурационных параметров безопасности требованиям безопасности в части соблюдения критериев, представляемых в политике безопасности в виде кортежей "Субъект-объект-уровень доступа", если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, и затем сравнивают множества зафиксированных конфигурационных параметров безопасности с указанными в выбранной политике безопасности в части подмножеств субъектов и объектов, рассчитывают для всех подтвержденных пар "субъект-объект", указанных в выбранной политике безопасности и зафиксированных в системе, действующие уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех текущих зафиксированных конфигурационных параметров безопасности и их значений, и затем сравнивают значения рассчитанных действующих уровней доступа с указанными в выбранном шаблоне или в политике безопасности, выявляя их различия, фиксируя состав и значения конфигурационных параметров, послуживших факторами влияния на отклонения уровней доступа, и составляя отчет

об анализе безопасности, содержащий описание выявленных ошибок администрирования системных и пользовательских программ и ресурсов, допущенных при реализации политики безопасности, по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных нарушений и факторов влияния на уровни доступа;

при этом в случае осуществления анализа соответствия конфигурационных параметров безопасности зафиксированному безопасному состоянию операционной среды информационной системы, если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, затем из множества ранее зафиксированных состояний безопасности информационной системы выбирают еще одно состояние, которое определяется как зафиксированное безопасное состояние, после чего сравнивают текущие конфигурационные параметры безопасности с указанными в зафиксированном безопасном состоянии по составу и значениям, рассчитывают для всех подтвержденных пар "субъект-объект", указанных в выбранном зафиксированном безопасном состоянии и зафиксированных в системе, действующие уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех текущих зафиксированных конфигурационных параметров безопасности и их значений, рассчитывают для тех же пар "субъект-объект" требуемые уровни доступа субъектов к объектам, учитывая воздействие на разрешения доступа всех конфигурационных параметров безопасности и их значений, указанных в зафиксированном безопасном состоянии, сравнивают рассчитанные действующие и требуемые уровни доступа и составляют отчет об анализе безопасности, содержащий описание выявленных отклонений от зафиксированных безопасных состояний операционной среды информационной системы по составу, значениям конфигурационных параметров безопасности и уровням доступа субъектов к объектам, перечень конфигурационных параметров безопасности и их значений, составляющих выявленные нарушения, и инструкции по изменению состава и значений конфигурационных параметров безопасности для устранения выявленных отклонений и факторов влияния на уровни доступа;

при этом в случае осуществления анализа соблюдения правил эффективного администрирования информационной системы, если для анализа выбрано текущее состояние, то взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируют состав и значения текущих конфигурационных параметров безопасности, или, если выбрано ранее зафиксированное состояние, то извлекают из него состав и значения зафиксированных конфигурационных параметров безопасности, оценивают по ним эффективность администрирования системы и объявляют ее эталонной, и после чего контролируют возникновение проблем управления системой, заключающихся в неэффективном администрировании системы, удаленно взаимодействуя со штатными программными средствами контроля и управления доступом операционной среды информационной системы, фиксируя состав и значения текущих конфигурационных

параметров безопасности, оценивая по ним текущую эффективность администрирования системы, выполняя сравнение эталонного значения эффективности администрирования системы с текущим, определяя численные характеристики, снижающие эффективность администрирования системы, и составляя отчет об анализе безопасности, содержащий описание проблем управления системой, заключающихся в неэффективном администрировании системы, график изменения эффективности администрирования системы с течением времени, перечень численных характеристик, снижающих эффективность, и рекомендации по повышению эффективности администрирования системы;

для устранения выявленных нарушений безопасности производят настройку конфигурационных параметров безопасности в соответствии с инструкциями, сформированными в отчетах о контроле безопасности или в отчетах об анализе безопасности, и составляют отчет о настройке безопасности, содержащий сведения об изменяемых конфигурационных параметрах безопасности и о результатах установки их значений;

периодически повторяют в необходимой последовательности вышеуказанные действия по настройке, фиксации, контролю и анализу конфигурационных параметров безопасности, составляют множество отчетов о контроле, анализе и настройке безопасности, тем самым непрерывно обеспечивая безопасность информационной системы.

2. Способ по п.1, отличающийся тем, что в качестве состояния информационной системы рассматривают все множество конфигурационных параметров безопасности, а именно субъекты, объекты и их атрибуты безопасности, состав которых определяется типом операционной среды информационной системы.

3. Способ по п.1, отличающийся тем, что типовые шаблоны безопасности составляют на основе рекомендаций экспертов по безопасной базовой настройке системных информационных ресурсов соответствующей операционной среды с учетом расширения области действия типовых шаблонов под влиянием политик безопасности, приводящим к появлению пользовательских информационных ресурсов помимо системных.

4. Способ по п.1, отличающийся тем, что политики безопасности составляют на основе корпоративных требований контроля и управления доступом, выдвигаемых к информационной системе, с учетом их выполнения в соответствующей операционной среде.

5. Способ по п.1, отличающийся тем, что в каждой рекомендации, составляющей типовой шаблон безопасности, образуют критерий безопасности системы, представляемый в виде кортежей "Состав конфигурационных параметров безопасности" или "Значение конфигурационного параметра безопасности", описывающих условия безопасности системы в виде множества конфигурационных параметров или их значений соответственно.

6. Способ по п.1, отличающийся тем, что в каждом правиле разграничения доступа, составляющем политику безопасности, образуют критерий безопасности системы, представляемый в виде кортежа "Субъект-объект-уровень доступа", описывающего отношение множеств субъектов, объектов и заданных для них уровней доступа, при выполнении которого система является безопасной.

7. Способ по п.1, отличающийся тем, что при составлении политики безопасности производят поиск противоречий в указанных уровнях доступа субъектов к объектам, определяя во множестве кортежей "Субъект-объект-уровень доступа" наличие

ограничений, заданных для одной пары "субъект-объект", но с разными уровнями доступа, с учетом иерархической структуры субъектов и иерархической структуры объектов, и для исключения обнаруженных противоречий формируют описание ошибок, допущенных при задании правил разграничения доступа субъектов к объектам на разных уровнях иерархии субъектов и объектов, а также производят коррекцию правил разграничения доступа соответствующей политики безопасности, исключая противоречивые правила или внося изменения в существующие правила и повторяя данную процедуру для всех правил до полного исключения противоречий.

8. Способ по п.1, отличающийся тем, что для настройки и контроля безопасности, осуществляемых в соответствии с типовым шаблоном безопасности, выполняют перечисление конфигурационных параметров, заданных в выбранном шаблоне безопасности, затем итеративно по каждому из перечисленных параметров взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и в случае осуществления настройки настраивают данный конфигурационный параметр безопасности системы либо в случае контроля безопасности фиксируют его наличие и текущее значение.

9. Способ по п.1, отличающийся тем, что для настройки безопасности, осуществляемой в соответствии с политикой безопасности, выполняют перечисление конфигурационных параметров, заданных в выбранной политике безопасности, затем итеративно по каждому из перечисленных параметров взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и настраивают данный конфигурационный параметр безопасности системы, при этом уровни доступа, указанные в политике безопасности, настраивают в виде прямых прав доступа, снимая остальные права, предоставляемые для каждой настраиваемой пары "субъект-объект" другими конфигурационными параметрами безопасности и их значениями.

10. Способ по п.1, отличающийся тем, для настройки безопасности, осуществляемой по зафиксированному шаблонному состоянию операционной среды информационной системы, выполняют перечисление конфигурационных параметров, заданных в выбранном зафиксированном шаблонном состоянии, затем итеративно по каждому из перечисленных параметров взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и настраивают данный конфигурационный параметр безопасности системы.

11. Способ по п.1, отличающийся тем, что для анализа безопасности, осуществляемого в соответствии с политикой безопасности, анализа соответствия конфигурационных параметров безопасности зафиксированному безопасному состоянию операционной среды информационной системы и анализа соблюдения правил эффективного администрирования информационной системы взаимодействуют со штатными программными средствами контроля и управления доступом операционной среды информационной системы и фиксируют текущие состав и значения всех конфигурационных параметров безопасности.

12. Способ по п.1, отличающийся тем, что численный показатель эффективности администрирования системы определяют как среднее количество записей контроля доступа, т.е. прав доступа, меток доступа и целостности, установленных для пользователей системы.

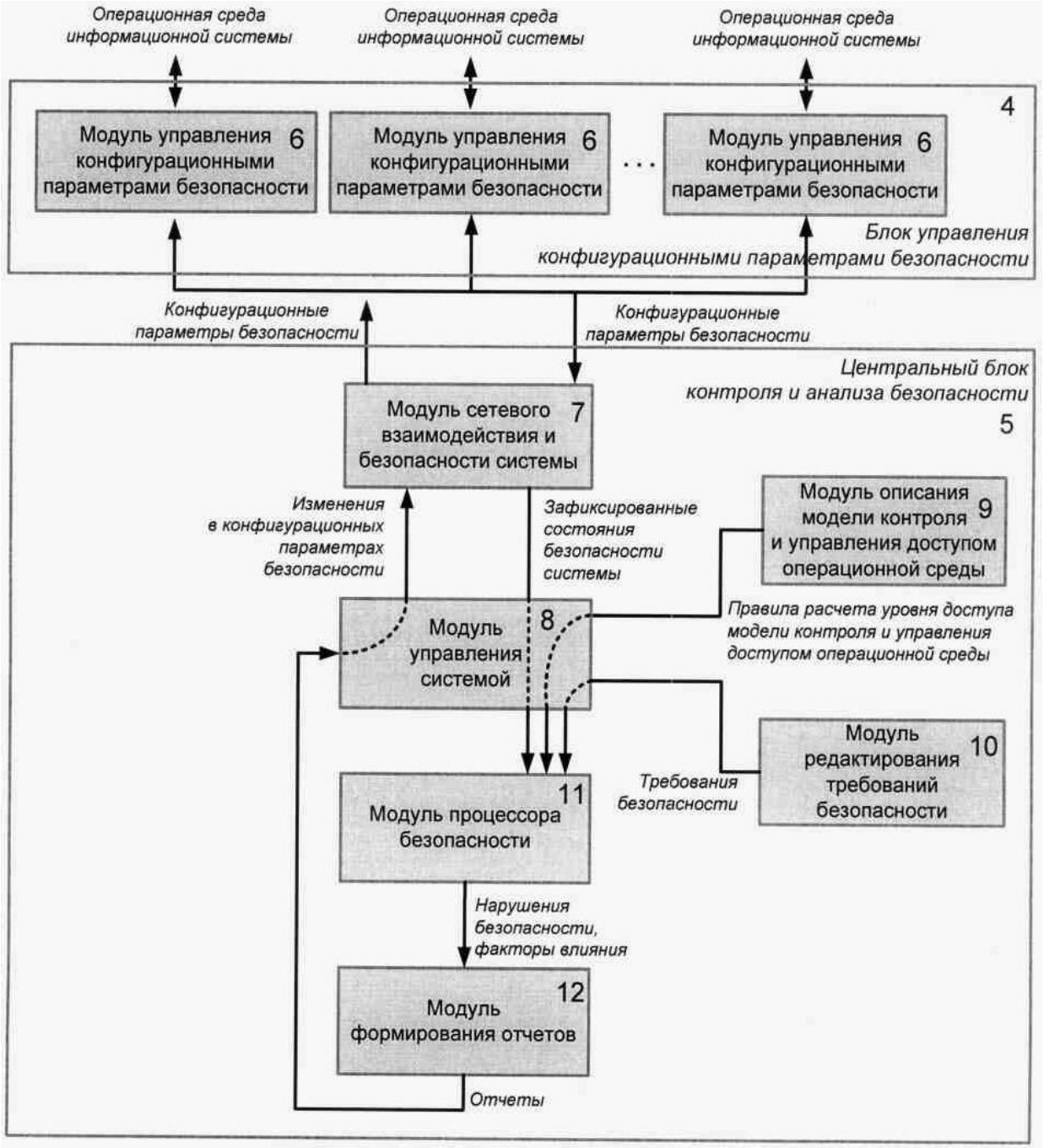
13. Способ по п.1, отличающийся тем, что расчет уровня доступа субъекта к объекту производят путем последовательного формирования множества доступных субъекту прав на основе прямых прав доступа объекта, заданных для конкретного

субъекта, с учетом прав, распространяющихся по иерархиям субъектов и объектов, т.е. с учетом унаследованных, групповых и прямых разрешений и запретов; прав, соответствующих конфигурационным параметрам безопасности; прав, соответствующих значениям конфигурационных параметров безопасности; прав, назначенных на зависимые объекты в информационной системе; прав, получаемых из меток доступа и целостности.

14. Система централизованной автоматизированной настройки, контроля и анализа безопасности информационных систем, включающая блок управления конфигурационными параметрами безопасности и центральный блок контроля и анализа безопасности, содержащий модуль управления системой, модуль сетевого взаимодействия и безопасности системы, модуль процессора безопасности и модуль формирования отчетов, отличающаяся тем, что в состав блока управления конфигурационными параметрами безопасности дополнительно включены модули, осуществляющие автоматизированную настройку конфигурационных параметров безопасности по заданным составу и значениям конфигурационных параметров безопасности, а также по уровням доступа субъектов к объектам, в совокупность модулей, образующих центральный блок, дополнительно включен модуль, обеспечивающий контроль целостности программного состава системы, идентификацию модулей управления конфигурационными параметрами безопасности и защиту передаваемых данных, в модуле управления системой дополнительно предусмотрено определение типа операционной среды информационной системы и подключение дополнительного модуля описания модели контроля и управления доступом операционной среды, интерактивное взаимодействие с дополнительно введенным модулем редактирования требований безопасности, а также каталогизированное хранение зафиксированных состояний, шаблонов безопасности, политик безопасности и формируемых отчетов; в модуле описания модели контроля и управления доступом операционной среды для соответствующего типа операционной среды дополнительно предусмотрено определение правил расчета уровней доступа субъекта к объекту на основе зафиксированного состояния операционной среды; в модуле процессора безопасности дополнительно предусмотрены функции расчета уровней доступа на множестве конфигурационных параметров безопасности, проверки выполнения условий безопасности системы, заданных в виде критериев из типовых шаблонов и политик безопасности, сопоставления зафиксированных состояний, оценки эффективности администрирования системы, выявления нарушений безопасности и их составов; в модуле формирования отчетов дополнительно предусмотрена возможность осуществления обратной связи через модуль управления и модуль сетевого взаимодействия и безопасности системы с модулями управления конфигурационными параметрами для осуществления настройки конфигурационных параметров безопасности с целью исправления обнаруженных нарушений безопасности.


1
Фиксация текущего состояния безопасности системы
Выбор зафиксированного состояния безопасности системы
2
Оценка эффективности администрирования системы
3
Определение проблем управления системой, заключающихся в неэффективном администрировании, и формирование их описаний
Отчет об анализе безопасности

Фиг. 2


Операционная среда информационной системы
Операционная среда информационной системы
Операционная среда информационной системы
4
Модуль управления конфигурационными параметрами безопасности 6
Модуль управления конфигурационными параметрами безопасности 6
Модуль управления конфигурационными параметрами безопасности 6
Блок управления конфигурационными параметрами безопасности
Конфигурационные параметры безопасности
Конфигурационные параметры безопасности
Центральный блок контроля и анализа безопасности 5
Модуль сетевого взаимодействия и безопасности системы 7
Изменения в конфигурационных параметрах безопасности
Зафиксированные состояния безопасности системы
Модуль описания модели контроля и управления доступом операционной среды 9
Правила расчета уровня доступа модели контроля и управления доступом операционной среды
Модуль управления системой 8
Модуль редактирования требований безопасности 10
Требования безопасности
Модуль процессора безопасности 11
Нарушения безопасности, факторы влияния
Модуль формирования отчетов 12
Отчеты

Фиг. 3