РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 571 372**(13) **C1**

(51) МПК
G06F 21/00 (2013.01)
G06F 12/14 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2014129423/08, 17.07.2014**

(24) Дата начала отсчета срока действия патента:
17.07.2014

Приоритет(ы):
(22) Дата подачи заявки: **17.07.2014**

(45) Опубликовано: **20.12.2015** Бюл. № **35**

(56) Список документов, цитированных в отчете о поиске: **RU 2504835 C1, 20.01.2014. RU 2207618 C2, 27.06.2003. RU 2444057 C1, 27.02.2012. EP 1303097 A2, 16.04.2003.**

Адрес для переписки:
170023, г.Тверь, а/я 2305, Ратовой Е.Н.

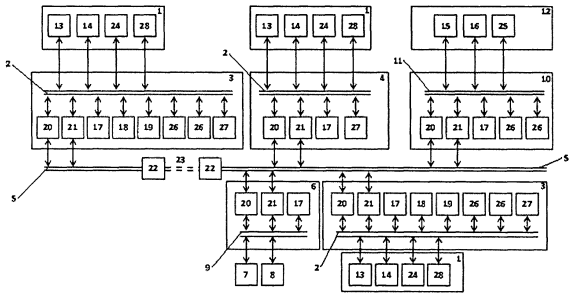
(72) Автор(ы):
Кочнев Валерий Васильевич (RU),
Семихина Людмила Александровна (RU),
Степанов Андрей Михайлович (RU),
Ефимов Алексей Юрьевич (RU),
Сазонов Андрей Юрьевич (RU),
Зуев Владимир Николаевич (RU)

(73) Патентообладатель(и):
Российская Федерация, от имени которой выступает государственный заказчик Министерство промышленности и торговли Российской Федерации (Минпромторг России) (RU)

(54) СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ

(57) Реферат:

Изобретение относится к защите от несанкционированного доступа к информации, хранимой на компьютерах, в автоматизированных системах обработки информации. Технический результат заключается в повышении защиты информации пользователя от несанкционированного доступа. Согласно изобретению система включает автоматизированные рабочие места пользователей (АРМ) и функциональные серверы системы, дополнительно введены системы обмена с внешними системами защиты информации, которые подключены соответственно к шинам управления и обмена данными АРМ пользователей и к шинам управления и обмена данными функциональных серверов, кроме того, в каждую систему защиты информации пользователя от несанкционированного доступа дополнительно введена база данных системы обмена с внешними системами защиты информации, соединенную с шиной управления и обмена данными соответствующего АРМ пользователя или функционального сервера. 1 ил.



RU 2571372 C1

RU 2571372 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 571 372**(13) **C1**

(51) Int. Cl.
G06F 21/00 (2013.01)
G06F 12/14 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2014129423/08, 17.07.2014**

(24) Effective date for property rights:
17.07.2014

Priority:
(22) Date of filing: **17.07.2014**

(45) Date of publication: **20.12.2015** Bull. № **35**

Mail address:
170023, g.Tver', a/ja 2305, Ratovoj E.N.

(72) Inventor(s):
Kochnev Valerij Vasil'evich (RU),
Semikhina Ljudmila Aleksandrovna (RU),
Stepanov Andrej Mikhajlovich (RU),
Efimov Aleksej Jur'evich (RU),
Sazonov Andrej Jur'evich (RU),
Zuev Vladimir Nikolaevich (RU)

(73) Proprietor(s):
Rossijskaja Federatsija, ot imeni kotoroj vystupaet gosudarstvennyj zakazchik Ministerstvo promyshlennosti i torgovli Rossijskoj Federatsii (Minpromtorg Rossii) (RU)

(54) SYSTEM FOR PROTECTING INFORMATION CONTAINING STATE SECRETS FROM UNAUTHORISED ACCESS

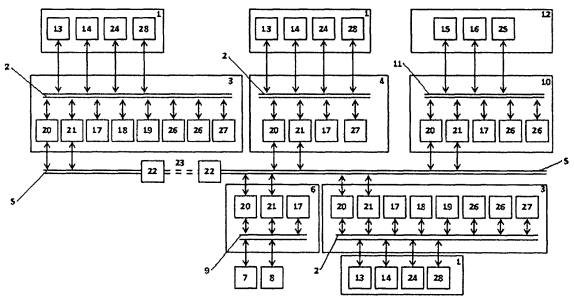
(57) Abstract:

FIELD: information technology.

SUBSTANCE: system includes user automated workstations and functional server systems, and additionally includes systems for communication with external information security systems, which are connected respectively to the control and data buses of the user automated workstations and to the control and data buses of the functional servers; furthermore, each system for protecting user information from unauthorised access further includes a database of the system for communication with external information security systems, connected to the control and data buses of the corresponding user automated workstation or functional server.

EFFECT: improved protection of user information from unauthorised access.

1 dwg



RU 2571372 C1

RU 2571372 C1

Изобретение относится к защите от несанкционированного доступа к информации, хранимой как на локальных компьютерах (автоматизированных рабочих местах пользователей или функциональных серверах), так и в вычислительной сети в целом, и может быть использовано в автоматизированных системах обработки информации, содержащей сведения, составляющие государственную тайну.

Современные автоматизированные системы создают на базе вычислительной сети, в которой все компьютеры домена автоматизированные рабочие места (АРМ) пользователей, функциональные серверы и сервер-контроллер домена - соединены друг с другом по сетевой магистрали.

Для комплексной защиты информации, содержащей сведения, составляющие государственную тайну, в автоматизированных системах необходимо обеспечить безопасность информации, хранящейся как на каждом локальном компьютере (АРМ пользователя или функциональном сервере), так и в вычислительной сети в целом. Кроме того, современным автоматизированным системам зачастую необходимо осуществлять защищенный обмен данными с другими автоматизированными системами, при этом распространенной ситуацией является использование во взаимодействующих автоматизированных системах различающихся классификаций мандатных меток.

Безопасность информации, содержащей сведения, составляющие государственную тайну, обеспечивают путем санкционированного доступа каждого пользователя в автоматизированной системе к разрешенным локальным и/или сетевым ресурсам - файлам, дискам, приложениям, принтерам.

Известна система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну (RU 2443017, кл. G06F 21/22, G06F 12/14, 2012 г.). включающая множество автоматизированных рабочих мест пользователей и функциональных серверов, по крайней мере, одно АРМ администратора безопасности информации и сервер-контроллер домена в компьютерной сети, которые соединены друг с другом по сетевой магистрали, множество систем защиты информации пользователя от несанкционированного доступа, каждая из которых содержит соответствующие агенты безопасности и систему разделения доступа пользователя, соединенные с шиной управления и обмена данными соответствующего АРМ пользователя или функционального сервера, систему защиты информации администратора от несанкционированного доступа, содержащую агент-администратор безопасности и систему разделения доступа администратора безопасности, соединенные с шиной управления и обмена данными соответствующего АРМ администратора безопасности информации, а также сервер безопасности и базу данных безопасности, подключенные к шине управления и обмена данными сервера-контроллера домена, при этом АРМ и функциональные серверы, сервер-контроллер домена и АРМ администратора безопасности информации содержат установленные на них аппаратно-программные модули доверенной загрузки, устройства криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства криптографической защиты информации, передаваемой по протоколу IP, которые подключены к шинам управления и обмена данными соответствующих АРМ и функциональных серверов, сервер-контроллера домена и АРМ администратора безопасности, все устройства криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства криптографической защиты информации, передаваемой по протоколу IP, соединены друг с другом по сетевой магистрали причем, по крайней мере, одно АРМ содержит установленные на него и подключенные к его шине управления и обмена данными

аппаратно-программный модуль доверенной загрузки, осуществляющий шифрование носителей информации, подключаемых по интерфейсу USB, и аппаратно-программный модуль доверенной загрузки, вырабатывающий и проверяющий электронную цифровую подпись.

Известная система защиты информации при использовании базовой операционной системы Windows XP Professional или операционной системы Windows 7 в вычислительной сети с активным каталогом (Active Directory) позволяет управлять безопасностью информации как на уровне сетевых ресурсов, так и на уровне файлов, папок и прав отдельных пользователей с помощью групп безопасности, прав пользователей и прав доступа на основе совместного использования дискреционных и мандатных правил разграничения доступа. Однако известная система защиты информации не обеспечивает требуемую защищенность в случае компрометации пароля или кражи смарткарты.

Наиболее близкой к предлагаемой является система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну (RU 2504835, кл. G06F 21/62, G06F 12/14, G06F 21/31, 2014 г), содержащая множество автоматизированных рабочих мест пользователей и функциональных серверов, по крайней мере, одно АРМ администратора безопасности информации и сервер-контроллер домена в компьютерной сети, которые соединены друг с другом по сетевой магистрали, множество систем защиты информации пользователя от несанкционированного доступа, каждая из которых содержит соответствующие агенты безопасности и систему разделения доступа пользователя, соединенные с шиной управления и обмена данными соответствующего АРМ пользователя или функционального сервера, систему защиты информации администратора от несанкционированного доступа, содержащую агент-администратор безопасности и систему разделения доступа администратора безопасности, соединенные с шиной управления и обмена данными соответствующего АРМ администратора безопасности информации, а также сервер безопасности и базу данных безопасности, подключенные к шине управления и обмена данными сервера-контроллера домена, при этом автоматизированные рабочие места и функциональные серверы, сервер-контроллер домена и АРМ администратора безопасности информации содержат установленные на них аппаратно-программные модули доверенной загрузки, устройства криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства криптографической защиты информации, передаваемой по протоколу IP, которые подключены к шинам управления и обмена данными соответствующих автоматизированных рабочих мест и функциональных серверов, сервер-контроллера домена и АРМ администратора безопасности, все устройства криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства криптографической защиты информации, передаваемой по протоколу IP, соединены друг с другом по сетевой магистрали, причем по крайней мере одно автоматизированное рабочее место содержит установленные на него и подключенные к его шине управления и обмена данными аппаратно-программный модуль доверенной загрузки, осуществляющий шифрование носителей информации, подключаемых по интерфейсу USB, и аппаратно-программный модуль доверенной загрузки, вырабатывающий и проверяющий электронную цифровую подпись, АРМ пользователей и АРМ администраторов безопасности информации содержат средства усиленной аутентификации, которые подключены соответственно к шинам управления и обмена данными автоматизированных рабочих мест и к шинам управления и обмена данными АРМ администраторов безопасности информации, а

каждая система защиты информации пользователя от несанкционированного доступа и система защиты информации администратора от несанкционированного доступа содержат соответствующую базу данных средств усиленной аутентификации пользователя и базу данных средств усиленной аутентификации администратора безопасности, соединенные соответственно с шиной управления и обмена данными соответствующего автоматизированного рабочего места пользователя или функционального сервера и с шиной управления и обмена данными АРМ администратора безопасности информации. Кроме того, сетевая магистраль имеет, по крайней мере, один разрыв, с каждой стороны которого включено по одному средству криптографической защиты информации, передаваемой по открытым каналам связи через неконтролируемую территорию

Однако известная система защиты информации от несанкционированного доступа также не обеспечивает возможности защищенного обмена информацией с внешними системами защиты информации, использующими отличающиеся классификации мандатных меток.

Задачей изобретения является разработка новой системы защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну на уровне операционной системы, на сетевом уровне и на уровне приложений, обеспечивающей реализацию аудита, контроля целостности программных файлов и данных, защиту от ввода/вывода на отчуждаемый носитель и обеспечивающей работу системы в замкнутой программной среде.

Техническим результатом изобретения является повышение эффективности по защите информации при передаче файлов во внешнюю систему защиты информации и обратного преобразования при получении файлов из внешней системы Поставленная задача и указанный технический результат достигаются тем, что система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну, содержит множество АРМ пользователей и функциональных серверов, по крайней мере, одно АРМ администратора безопасности информации и сервер-контроллер домена в компьютерной сети, которые соединены друг с другом по сетевой магистрали, множество систем защиты информации пользователя от несанкционированного доступа, каждая из которых содержит соответствующие агент безопасности и систему разделения доступа пользователя, соединенные с шиной управления и обмена данными соответствующего АРМ пользователя или функционального сервера, систему защиты информации администратора от несанкционированного доступа, содержащую агент-администратор безопасности и систему разделения доступа администратора безопасности, соединенные с шиной управления и обмена данными соответствующего АРМ администратора безопасности информации, а также сервер безопасности и базу данных безопасности, подключенные к шине управления и обмена данными сервера-контроллера домена, при этом АРМ и функциональные серверы, сервер-контроллер домена и АРМ администратора безопасности информации содержат установленные на них аппаратно-программные модули доверенной загрузки, устройства криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства криптографической защиты информации, передаваемой по протоколу IP, которые подключены к шинам управления и обмена данными соответствующих АРМ и функциональных серверов, сервер-контроллера домена и АРМ администратора безопасности, все устройства криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства

криптографической защиты информации, передаваемой по протоколу IP, соединены друг с другом по сетевой магистрали, причем, по крайней мере, одно АРМ содержит установленные на него и подключенные к его шине управления и обмена данными аппаратно-программный модуль доверенной загрузки, осуществляющий шифрование носителей информации, подключаемых по интерфейсу USB, и аппаратно-программный модуль доверенной загрузки, вырабатывающий и проверяющий электронную цифровую подпись, АРМ пользователей и в АРМ администраторов безопасности информации содержат средства усиленной аутентификации, которые подключены соответственно к шинам управления и обмена данными АРМ и к шинам управления и обмена данными АРМ администраторов безопасности информации, каждая система защиты информации пользователя от несанкционированного доступа и система защиты информации администратора от несанкционированного доступа содержат соответствующую базу данных средств усиленной аутентификации пользователя и базу данных средств усиленной аутентификации администратора безопасности, соединенные соответственно с шиной управления и обмена данными соответствующего АРМ пользователя или функционального сервера и с шиной управления и обмена данными АРМ администратора безопасности информации, при этом сетевая магистраль имеет, по крайней мере, один разрыв, с каждой стороны которого включено по одному средству криптографической защиты информации, передаваемой по открытым каналам связи через неконтролируемую территорию. Согласно изобретению в АРМ пользователей и функциональные сервера дополнительно введены системы обмена с внешними системами защиты информации, которые подключены соответственно к шинам управления и обмена данными АРМ пользователей и к шинам управления и обмена данными функциональных серверов, кроме того, в каждую систему защиты информации пользователя от несанкционированного доступа дополнительно введены соответствующие базы данных системы обмена с внешними системами защиты информации, соединенные соответственно с шиной управления и обмена данными соответствующего автоматизированного рабочего места пользователя или функционального сервера.

Предлагаемая система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну, обеспечивает защиту информации в автоматизированной системе на уровне операционной системы, на сетевом уровне и на уровне приложений, реализацию аудита, контроля целостности программных файлов и данных, защиты от ввода/вывода на отчуждаемый носитель, обеспечения работы в замкнутой программной среде путем совместного использования дискреционных и мандатных правил разграничения доступа, выполнения идентификации и аутентификации пользователей с применением подключаемых дополнительных устройств усиленной идентификации и аутентификации, а также обмена информацией с внешними системами защиты информации, использующими отличающиеся классификации мандатных меток. Это и обеспечивает положительный технический результат - возможность защищенного обмена информации с внешними системами защиты информации с сохранением мандатных атрибутов передаваемых файлов за счет преобразования мандатных меток в процессе обмена к классификации внешней системы защиты информации при передаче файлов во внешнюю систему защиты информации и обратного преобразования при получении файлов из внешней системы.

На фиг. 1 представлена структурная схема системы защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну.

Система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну, содержит множество АРМ 1 пользователей с системой защиты информации от несанкционированного доступа, связанными шиной 2 управления и обмена данными с АРМ 3 и функциональными серверами 4 в компьютерной сети, соединенные друг с другом по сетевой магистрали 5, к которой подключен сервер-контроллер 6 домена, сервер 7 безопасности и база 8 данных сервера 7 безопасности, подключенные в свою очередь к шине 9 управления и обмена данными сервера-контроллера 6 домена. Система содержит также, по крайней мере, одно автоматизированное рабочее место 10 администратора безопасности информации, подключенное к сетевой магистрали 5, имеющее внутреннюю шину 11 управления и обмена данными, и, по крайней мере, одну систему 12 защиты информации администратора. Каждое АРМ 1 защиты информации пользователя от несанкционированного доступа содержит агент 13 безопасности и систему 14 разделения доступа пользователя, соединенные с шиной 2 управления и обмена данными соответствующего АРМ 1 или функционального сервера 4, а система 12 защиты информации администратора от несанкционированного доступа содержит агент-администратор 15 безопасности и систему 16 разграничения доступа администратора безопасности, соединенные с шиной 11 управления и обмена данными соответствующего АРМ 10 администратора безопасности информации. Кроме того, АРМ 3 и функциональные серверы 4, сервер-контроллер 6 домена и АРМ 10 администраторов безопасности информации содержат установленные на них аппаратно-программные модули 17 доверенной загрузки, а также устройства 20 криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства 21 криптографической защиты информации, передаваемой по протоколу IP, которые подключены соответственно к шинам 2 управления и обмена данными АРМ 3 и функциональных серверов 4, к шине 9 управления и обмена данными сервера-контроллера 6 домена и к шинам 11 управления и обмена данными АРМ 10 администраторов безопасности информации. Все устройства 20 криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства 21 криптографической защиты информации, передаваемой по протоколу IP, соединены друг с другом по сетевой магистрали 5. По крайней мере, одно АРМ 3 содержит установленные на него и подключенные к его шине 2 управления и обмена данными аппаратно-программный модуль 18 доверенной загрузки, осуществляющий шифрование носителей информации, подключаемых по интерфейсу USB, и аппаратно-программный модуль 19 доверенной загрузки, вырабатывающий и проверяющий электронную цифровую подпись. Сетевая магистраль 5 имеет, по крайней мере, один разрыв, с каждой стороны которого включено по одному средству 22 криптографической защиты информации, передаваемой по открытым каналам связи через неконтролируемую территорию 23. Каждое АРМ 1 с защитой информации пользователя от несанкционированного доступа содержит соответствующую базу 24 данных средств усиленной аутентификации пользователя, соединенную с шиной 2 управления и обмена данными соответствующего АРМ 3 пользователя или функционального сервера 4, а система 12 защиты информации администратора от несанкционированного доступа содержит базу 25 данных средств усиленной аутентификации администратора безопасности, соединенную с шиной 11 управления и обмена данными соответствующего АРМ 10 администратора безопасности информации. АРМ 3 и АРМ 10 администраторов безопасности информации содержат средства 26 усиленной аутентификации, которые подключены соответственно к шинам

2 управления и обмена данными АРМ 3 и к шинам 11 управления и обмена данными АРМ 10 администраторов безопасности информации. АРМ 3 и функциональные серверы 4 содержат систему 27 обмена с внешними системами защиты информации, которые подключены соответственно к шинам 2 управления и обмена данными АРМ 3 и функциональных серверов 4, а каждое рабочее место 1 с системой защиты информации пользователя от несанкционированного доступа содержит базу 28 данных системы обмена с внешними системами защиты информации, соединенную с шиной 2 управления и обмена данными соответствующего автоматизированного рабочего места 1 и 3 пользователя или функционального сервера 4.

В состав системы защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну, могут быть включены несколько АРМ 10 администраторов безопасности информации и несколько соответственно соединенных с их шинами 11 управления и обмена данными агентов-администраторов 15 безопасности. В этом случае каждый из администраторов безопасности информации может оперативно контролировать работу пользователей в сети. При необходимости контроля работы администраторов безопасности с шинами 11 управления и обмена данными соответствующих АРМ 10 администраторов безопасности информации соединяют соответствующие агенты 13 безопасности.

Работает предлагаемая система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну, следующим образом.

Входящие в состав АРМ 1 с системой защиты информации пользователя от несанкционированного доступа агенты 13 безопасности, входящие в состав систем 12 защиты информации администратора от несанкционированного доступа агенты-администраторы 15 безопасности, а также подключенные к шине 9 управления и обмена данными сервера-контроллера 6 домена сервер 7 безопасности и база 8 данных безопасности образуют систему контроля и управления профилями.

Входящие в состав АРМ 1 с системой защиты информации пользователя от несанкционированного доступа системы 14 разделения доступа пользователя, а также входящие в состав систем 12 защиты информации администратора от несанкционированного доступа системы 16 разделения доступа администратора безопасности образуют систему разграничения доступа.

Входящие в состав АРМ 1 с системой защиты информации пользователя от несанкционированного доступа базы 17 данных средств усиленной аутентификации пользователя, а также входящие в состав систем 12 защиты информации администратора от несанкционированного доступа базы 18 данных средств усиленной аутентификации администратора безопасности образуют систему дополнительной защиты информации.

Система контроля и управления профилями выполняет следующие функции: управление профилями безопасности пользователей, групп пользователей и компьютеров; разграничение доступа пользователей к функциям программы "Проводник" (команда "Выполнить", панель

управления, панель задач в меню "Пуск", настройка дисплея и т.д.); определение списка разрешенных для запуска приложений (обеспечение замкнутой программной среды) путем формирования пользовательского меню в программе "Проводник" и контроль запуска несанкционированных приложений; контроль состояния компьютеров в сети, сбор статистики работы (время старта, время непрерывной работы); контроль сеанса работы интерактивных пользователей и сетевых пользователей, получивших доступ к разделяемым ресурсам; протоколирование действий администратора

безопасности информации и пользователей; разграничение полномочий администраторов безопасности информации на АРМ 10 администраторов безопасности информации (оператор, администратор); оповещение администратора безопасности информации о попытках несанкционированного доступа, нарушениях работы комплексной системы защиты информации от несанкционированного доступа и других критических ситуациях в сети.

Система контроля и управления профилями реализует функции по разграничению доступа к приложениям (программам), запускаемым на АРМ 3 и функциональных серверах 4, регистрации событий защиты (аудит), контролю целостности программных файлов и данных, защите от ввода/вывода на отчуждаемый носитель.

Входными данными для системы контроля и управления профилями являются: информация о составе зарегистрированных пользователей в центральной базе 8 данных безопасности автоматизированной системы (на контроллере домена), записи в системных журналах и журналах безопасности в АРМ 3 пользователя или функциональном сервере 4 и команды администратора безопасности информации.

Выходными данными системы контроля и управления профилями являются протоколы действий администраторов на АРМ 10 администраторов безопасности информации и событий-попыток несанкционированного доступа к информации, контроля целостности, работы с внешними носителями в автоматизированной системе, информация о состоянии компьютеров, служб, приложений и настройках политики безопасности.

Система контроля и управления профилями использует объектную идеологию, т.е. вся структура компьютерной сети и управляющая информация представлена в виде объектов управления. Все устройства оперируют с объектами управления (объектами SMS). Все объекты управления хранятся в базе 8 данных сервера безопасности.

База 8 данных сервера безопасности содержит основной корневой объект управления, который содержит в себе такие объекты управления, как домены или рабочие группы базовой операционной системы, содержащие в свою очередь такие объекты, как компьютеры, пользовательские приложения, профили пользователей, профили групп пользователей, профили безопасности и устройства (дисководы, порты и т.д.).

Каждый объект управления характеризуют основные атрибуты и свой специфический набор дополнительных атрибутов, методов доступа и управления этим объектом управления.

Сервер 7 безопасности обеспечивает синхронизацию объектов управления с агентами 13 безопасности, агентами-администраторами 15 безопасности и другими серверами 7 безопасности: установление логических соединений с агентами 13 безопасности и агентами-администраторами 15 безопасности, проверку наличия логических соединений с агентами 13 безопасности и агентами-администраторами 15 безопасности, прием и обработку запросов от агента-администратора 15 безопасности на добавление/исключение объектов управления в базе данных профилей и модификацию их атрибутов, прием и обработку запросов от агентов 13 безопасности на получение профиля пользователя и составе доступных ему приложений, формирование ответов на эти запросы, прием и обработку сообщений от агентов 13 безопасности и агентов-администраторов 15 безопасности, при появлении событий - попыток несанкционированного доступа к информации в системных журналах агентов 13 безопасности, ведение протокола действий администраторов безопасности на АРМ 10 администраторов безопасности информации в части контроля и управления профилями.

Между сервером 7 безопасности, агентами 13 безопасности и агентами-

администраторами 15 безопасности устанавливаются логические соединения. Каждое установленное логическое соединение имеет свой идентификатор, что позволяет серверу 7 безопасности определять, с какими агентами 13 безопасности или агентами-администраторами 15 безопасности производится обмен информацией. При успешном установлении соединения ему присваивается идентификатор, а агентам 13 безопасности или агентам-администраторам 15 безопасности посылается соответствующее сообщение.

Сервер 7 безопасности производит проверку наличия логических соединений с агентами 13 безопасности и агентами-администраторами 15 безопасности по таймеру. Запрос на разрыв соединения с сервером 7 безопасности посылают агенты 13 безопасности или агенты-администраторы 15 безопасности. При этом соединение удаляется из базы 8 данных сервера безопасности.

После установления соединения сервер 7 безопасности, агенты 13 безопасности и агенты-администраторы 15 безопасности обмениваются сообщениями, содержащими запросы и ответы.

Агенты 13 безопасности посылают серверу 7 безопасности следующие типы запросов: информация о базовой операционной системе, на разрыв соединения, на проверку соединения, на перечисление приложений пользователя, на получение профиля пользователя, на обработку события на компьютере, на получение устройств компьютера, на получение списка файлов для проверки. При этом агентами 13 безопасности передается информация о компьютере, текущем пользователе и событиях, а сервер 7 безопасности передает агентам 13 безопасности информацию о профилях, о составе приложений, проверяемых файлов и устройств.

Агенты-администраторы 15 безопасности посылают серверу 7 безопасности следующие типы запросов: на регистрацию соединения, на перечисление доменов, на добавление домена, на удаление домена, на перечисление компьютеров домена, на добавление компьютера, на удаление компьютера, на перечисление приложений домена, на добавление приложения, на удаление приложения, на перечисление пользователей домена, на добавление пользователя, на удаление пользователя, на изменение состояния компьютера в базе, на изменение свойств пользователя, на изменение свойств компьютера, на изменение свойств домена, на изменение свойств приложения, на удаленное управление компьютером, на перечисление групп пользователей, на добавление группы пользователей, на удаление группы пользователей, на изменение свойств группы пользователей, на запись протокола работы администратора, на чтение протокола работы администратора, на получение списка запущенных приложений, на завершение приложения, на очистку протокола работы администратора, на очистку тревоги, на установку свойств группе пользователей, на чтение протокола событий, на перечисление профилей безопасности, на добавление профиля безопасности, на удаление профиля безопасности, на изменение свойств профиля безопасности, на перечисление устройств, на изменение свойств устройства, на добавление устройства, на удаление устройства, на изменение списка файлов для проверки, на очистку протокола событий, на получение свойств ГМД (флеш-памяти, ЛД), на чтение архива, протокола событий, на чтение архива протокола работы.

Сервер 7 безопасности производит опрос состояния агентов 13 безопасности (о составе запущенных приложений, текущем пользователе), а также осуществляет перезагрузку, выключение компьютеров, выход из системы, запуск/останов приложений. Сервер 7 безопасности передает агенту-администратору 15 безопасности запросы о состоянии компьютеров агентов безопасности, составе запущенных приложений, запуске приложения и о происшедших событиях.

Агент 13 безопасности выполняет следующие функции: контроль состояния автоматизированного рабочего места пользователя или функционального сервера, контроль состояния сеанса интерактивного пользователя, настройку рабочей среды пользователя и установление ограничений, слежение за состоянием приложений и процессов, слежение за содержимым системных журналов, выполнение команд от имени администратора безопасности (перезагрузку, запуск/останов приложений, блокировку системы). Агент 13 безопасности устанавливает соединение (регистрацию) с сервером 7 безопасности и затем периодически отправляет серверу 7 безопасности запрос на проверку наличия соединения и обрабатывает ответ. Взаимодействие с сервером 7 безопасности после установления логического соединения осуществляется на основе запрос-ответного механизма. Агент 13 безопасности отвечает за контроль событий-попыток несанкционированного доступа к информации, сбор статистической информации (имя пользователя, время начала и завершения сеанса работы пользователя, время включения и выключения компьютера и т.д.), информации о состоянии задач и запущенных процессов, контроль целостности файлов на автоматизированном рабочем месте пользователя или функциональном сервере. Агент 13 безопасности выполняет управляющие команды, поступившие от агента-администратора 15 через сервер 7 безопасности по сети, и передает серверу 7 безопасности информацию о компьютере, о текущем пользователе, профилях, составе приложений, результатах контроля целостности проверяемых файлов и о событиях-попытках несанкционированного доступа к информации. Агент 13 безопасности после установления логического соединения с сервером 7 безопасности получает от него сообщение с системной политикой компьютера. Серверу 7 безопасности передается информация о типе базовой операционной системы.

При входе пользователя в систему агент 13 безопасности передает серверу 7 безопасности информацию о пользователе (имя пользователя, время начала сеанса). Сервер 7 безопасности передает информацию о системной политике для пользователя. При установке системной политики компьютера и пользователя агент 13 безопасности изменяет значения в реестре. Далее агент 13 безопасности формирует и посылает серверу 7 безопасности запросы на перечисление приложений пользователя, на получение профиля, на получение устройств компьютера и списка файлов для проверки. К приложениям пользователя относятся основные исполняемые модули, запускаемые через меню "Пуск", и вспомогательные исполняемые модули, запускаемые из основных приложений. Ответы от сервера 7 безопасности обрабатываются агентом 13 безопасности, производится установка профиля пользователя в реестре, состава ему доступных основных приложений в меню "Пуск" и состава вспомогательных приложений, запускаемых из основных приложений. Агент 13 безопасности производит контроль целостности путем вычисления контрольных сумм файлов системы защиты информации, системных и пользовательских файлов и сравнение их с соответствующими эталонными значениями. Функция контроля целостности позволяет обнаруживать любое изменение (удаление, добавление, замену) данных файла и файловой структуры в целом. Контроль целостности производится путем вычисления имитовставки. При изменении контрольных сумм файлов или отсутствии какого-либо файла формируется сообщение для сервера 7 безопасности о нарушении целостности. Агент 13 безопасности осуществляет контроль над процессами, работающими в системе. Производится сбор информации о файлах-процессах, поиск окон процессов и передача информации о процессах серверу 7 безопасности. Осуществляется запуск и остановка процессов по запросу от сервера 7 безопасности, формируемому в свою очередь по команде агента-

администратора 15 безопасности. Агент 13 безопасности осуществляет контроль за системными событиями путем слежения за содержимым системных журналов и при появлении событий-попыток несанкционированного доступа к информации и других критических событий, передает сообщения об их возникновении серверу 7 безопасности. Агент 13 безопасности выполняет контроль запуска всех приложений и определяет, относится основное или вспомогательное приложение к числу разрешенных для запуска. Если нет, то приложение не запускается, а серверу 7 безопасности передается сообщение о событии-попытке несанкционированного доступа к информации. Кроме того, агент 13 безопасности производит контроль сообщений о начале работы системы разграничения доступа. При успешном начале работы системы разграничения доступа в реестре сохраняются соответствующие настройки. В противном случае осуществляется восстановление настроек системы разграничения доступа в реестре и перезапуск компьютера. Если восстановление не приводит к успешному запуску системы разграничения доступа, то создается запись для администратора о неуспешном восстановлении системы и блокируется инициализация агента 13 безопасности. Агент 13 безопасности выполняет контроль установки внешних носителей информации по сообщениям от монитора файловой системы (drivemon.sys) о монтировании тома. Далее агент 13 безопасности формирует запрос о профиле безопасности (дескрипторе) устройства серверу 7 безопасности. После получения профиля безопасности система разграничения доступа производит контроль доступа пользователя, работающего на компьютере, к устройству. При разрешении доступа осуществляются операции с внешним носителем информации. После этого доступ к устройству закрывается. При копировании на носитель факт копирования передается серверу 7 безопасности. Сервер 7 безопасности передает факты выполнения операций с носителем информации, в том числе события-попытки несанкционированного доступа к информации, на автоматизированных рабочих местах 10 администраторов безопасности информации в журнал регистрации.

Агент-администратор 15 безопасности выполняет следующие функции: ведение базы данных сервера безопасности (создание, изменение, удаление объектов), мониторинг состояния объектов (компьютеров, приложений), управление компьютером и сеансами работы пользователей, протоколирование действий администраторов и операторов, вывод на экран и печать протоколов действий администраторов и операторов. Агент-администратор 15 безопасности является основным модулем для осуществления управляющих функций, задания основных параметров и мониторинга событий в сети. Агент-администратор 15 безопасности взаимодействует с сервером 7 безопасности. В обмене участвует управляющая и настроечная информация о задачах, процессах и событиях на автоматизированных рабочих местах 3 пользователей или функциональных серверах 4. Отображение информации и интерфейс с пользователем осуществляются в графическом виде. При включении агента-администратора 15 безопасности производится инициализация процесса установления соединения (регистрации) с сервером 7 безопасности. Агент-администратор 15 безопасности формирует запрос на регистрацию (установление) соединения с сервером 7 безопасности и обрабатывает ответ. Периодически агент-администратор 15 безопасности отправляет серверу 7 безопасности запрос на проверку наличия соединения и обрабатывает ответ. Взаимодействие агента-администратора 15 безопасности с сервером 7 безопасности после установления логического соединения, в основном, осуществляется на основе запрос - ответного механизма.

Агент-администратор 15 реализует следующие группы функций.

Группа функций по работе с объектами базы 8 данных сервера 7 безопасности позволяет агенту-администратору 15 формировать запросы для сервера 7 безопасности на получение списка объектов, на добавление, удаление и изменение свойств объектов (доменов, компьютеров, пользователей, групп пользователей, приложений, профилей безопасности). Запросы формируются по команде администратора 15 безопасности посредством графического интерфейса и обрабатываются полученные ответы. В оперативной памяти хранится информация о составе и состоянии управляемых объектов, их атрибутов и параметров, аналогичная информации в базе 8 данных сервера безопасности.

При получении ответа от сервера 7 безопасности изменяется состояние базы 8 данных в оперативной памяти АРМ 10 администратора безопасности информации. Хранение объектов в оперативной памяти позволяет повысить быстродействие операций по графическому отображению состояния объектов. Например, для компьютера к этой группе функций относятся: запросы/ответы на получение списка компьютеров домена, на добавление компьютера, удаление компьютера, изменение свойств компьютера.

Группа функций по работе с протоколом (журналом) событий позволяет обрабатывать запросы/ответы на просмотр и очистку протокола событий, на получение архива протокола событий.

Группа функций по работе с протоколом (журналом) работы администратора безопасности информации позволяет обрабатывать запросы/ответы на просмотр и очистку протокола работы администратора 15 безопасности информации, на получение архива протокола работы администратора 15 безопасности информации.

Группа функций по управлению компьютером обеспечивает формирование запросов серверу 7 безопасности и обработку ответов на получение информации, списке запущенных приложений, удаленную перезагрузку, выключение компьютера или выход из системы, удаленный

запуск приложения, формирование запросов на удаленное завершения приложения, на получение информации о текущем пользователе компьютера.

Группа функций по обработке запросов от сервера 7 безопасности о состоянии объектов обеспечивает обработку и отображение информации об изменении состояния компьютеров, запуске приложений пользователями, событиях-попытках несанкционированного доступа к информации.

Группа функций по контролю целостности предназначена для формирования запросов серверу 7 безопасности и обработку ответов на получение или изменение списка файлов для проверки контрольных сумм для компьютеров домена.

Система разграничения доступа является дополнением встроенной в базовую операционную систему системы безопасности мандатной моделью доступа, подразумевающей наличие для каждого субъекта и объекта доступа иерархических атрибутов (грифа секретности) и неиерархических атрибутов (категорий доступа).

Основным принципом работы системы безопасности базовой операционной системы является сосредоточение центральных процедур проверки прав доступа в мониторе безопасности, являющемся составной частью ядра базовой операционной системы. Функции монитора безопасности вызываются менеджером объектов базовой операционной системы при обращении к любому системному объекту с целью подтверждения полномочий обращающегося субъекта. При этом в монитор безопасности передается вся информация, необходимая для анализа атрибутов безопасности субъекта и объекта доступа.

Основным методом изменения системы безопасности базовой операционной системы

в предлагаемой системе разграничения доступа является перехват функции проверки прав доступа в мониторе безопасности и дополнение описателей безопасности объектов и субъектов доступа мандатными атрибутами без нарушения внутренней структуры описателей. При этом сопоставление описателя объекту, его хранение и ограничение доступа к нему реализуется стандартными функциями базовой операционной системы.

В описатель безопасности субъекта доступа (маркер доступа, Token) мандатные атрибуты заносятся на этапе регистрации пользователя в системе и находятся в специально отмеченных элементах списка групп, к которым принадлежит пользователь. Эти атрибуты состоят из грифа секретности, представляемого предопределенным при создании системы идентификатором безопасности (SID), и нескольких категорий доступа, каждая из которых представляется идентификатором безопасности определенных в агентстве безопасности групп пользователей (такие идентификаторы уникальны для каждого агентства). Хранение этой информации производится в базе 8 данных системы безопасности базовой операционной системы, при этом каждому пользователю системы соответствует несколько записей в базе 8 данных: базовая запись, содержащая стандартные атрибуты пользователя в базовой операционной системе, и по одной записи для каждого грифа секретности, к работе с которым допущен пользователь, содержащей список категорий для соответствующего грифа и пользователя.

В описателе безопасности (дескрипторе защиты) объекта доступа (Security Descriptor) мандатные атрибуты заносятся в дискреционный список доступа (Discretionary Access Control List, DACL) в виде специально отмеченных элементов (Access Control Element, ACE), при этом идентификаторы безопасности этих элементов соответствуют описанным выше. Хранение описателей безопасности объектов доступа возлагается на системы 14 разделения доступа пользователей и на систему 16 разделения доступа администратора безопасности.

Система разграничения доступа реализует алгоритм проверки прав доступа, созданный на базе стандартного алгоритма монитора безопасности и дополненный проверкой мандатных атрибутов объекта и субъекта.

Обработка мандатных атрибутов субъекта и объекта осуществляется по следующим правилам:

Субъект имеет доступ к объекту, если все перечисленные в описателе безопасности (дескрипторе защиты) объекта категории доступа входят в маркер доступа субъекта.

Субъект имеет доступ по чтению и изменению объекта, если гриф секретности объекта имеет значение не более грифа секретности субъекта.

Если гриф секретности объекта больше грифа секретности субъекта и объект является контейнерным (содержит другие объекты), субъект имеет доступ на добавление в объект подобъектов.

Если доступ разрешен в соответствии только с мандатными правилами разграничения доступа, но не разрешен по дискреционным (или наоборот), Доступ запрещается.

Аппаратно-программные модули 17 доверенной загрузки, аппаратно-программные модули 18 доверенной загрузки, осуществляющие шифрование носителей информации, подключаемых по интерфейсу USB, и аппаратно-программные модули 19 доверенной загрузки, вырабатывающие и проверяющие электронную цифровую подпись, обеспечивают контроль целостности файловой системы АРМ 3 и функциональных серверов 4, а так же порядок загрузки программного обеспечения на них в соответствии с выбранным уровнем доступа к информации.

Устройства 20 криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства 21 криптографической защиты

информации, передаваемой по протоколу IP, обеспечивают шифрование информации, передаваемой по сетевой магистрали 5 между АРМ 3, функциональными серверами 4, сервером-контроллером 6 домена и АРМ 10 администраторов безопасности информации.

Средство 22 криптографической защиты информации, передаваемой по открытым каналам связи, обеспечивает шифрование информации при передаче ее через участки, выходящие за пределы контролируемой зоны 23.

Система дополнительной защиты информации является дополнением встроенной в базовую операционную систему модифицированной системы безопасности, реализующей алгоритм проверки прав доступа, созданный на базе стандартного алгоритма монитора безопасности и дополненный проверкой мандатных атрибутов объекта и субъекта.

Система дополнительной защиты информации при входе пользователя в систему реализует дополнительный алгоритм его аутентификации с помощью средств 26 усиленной аутентификации (биометрических датчиков, ключевых носителей, считывателей смарткарт и т.п.).

Для этого к стандартным элементам модифицированной системы безопасности добавляют «библиотеку расширения базовой системы идентификации и аутентификации пользователя», хранение аутентификационных данных для которой возлагается на базы 24 данных средств усиленной аутентификации пользователя и базу 25 данных средств усиленной аутентификации администратора безопасности.

При входе пользователя в систему соответствующий агент 13 безопасности и агент-администратор 15 безопасности с помощью хранящегося в соответствующей базе 24 данных средств усиленной аутентификации пользователя и в базе 25 данных средств усиленной аутентификации администратора безопасности проверяют, установлены ли и разрешены ли на запуск дополнительные системы защиты информации (средства 26 усиленной аутентификации), и при положительном результате они выдают команды на проверку аутентификационной информации средствам 26 усиленной аутентификации (биометрическим датчикам, ключевым носителям, считывателям смарткарт и т.п.).

После успешной аутентификации пользователя средствами 26 усиленной аутентификации информация о пользователе передается в систему контроля и управления профилями для дальнейшей штатной работы.

Удобство использования средств 26 усиленной аутентификации обусловлено отсутствием необходимости запоминания пользователем сложных паролей, т.к. используются технические средства 26 усиленной аутентификации (биометрические датчики, ключевые носители, считыватели смарткарт и т.п.).

Система 27 обмена с внешними системами защиты информации осуществляет передачу файлов между системами защиты информации с сохранением мандатных атрибутов пересылаемых файлов.

Для осуществления обмена информацией во внешней системе защиты информации также должна содержаться система 27 обмена с внешними системами защиты информации.

Поскольку классификации мандатных меток в различных системах защиты информации могут различаться, мандатные метки файла одной системы защиты информации могут оказаться неприменимы в другой системе защиты информации. Для сохранения мандатных атрибутов пересылаемых файлов система 27 обмена с внешними системами защиты информации осуществляет преобразование мандатных меток передаваемых файлов к виду, используемому во внешней системе защиты информации. Преобразование выполняется в соответствии с набором правил, содержащихся в базе 28 данных системы обмена с внешними системами защиты. Правила представляют

собой набор соответствий грифов секретности категорий доступа системы защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну, грифам секретности и категориям доступа одной или нескольких внешних систем защиты информации.

Передача информации выполняется следующим образом - мандатная метка пересылаемого файла считывается и преобразуется в соответствии с правилами, заданными в базе 28 данных системы обмена с внешними системами защиты. Файл и его преобразованная метка пересылаются и сохраняются во внешнюю систему защиты информации.

Передача файла в обратную сторону выполняется аналогично.

При использовании предлагаемой системы защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну, достигается возможность защищенного обмена информацией с внешними системами защиты информации, использующими отличающиеся классификации мандатных меток, за счет преобразования мандатных меток в процессе обмена к классификации внешней системы защиты информации при передаче файлов во внешнюю систему защиты информации и обратного преобразование при получении файлов из внешней системы.

Формула изобретения

Система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну, включающая множество автоматизированных рабочих мест пользователей и функциональных серверов, по крайней мере, одно автоматизированное рабочее место администратора безопасности информации и сервер-контроллер домена в компьютерной сети, соединенные друг с другом по сетевой магистрали, множество систем защиты информации пользователя от несанкционированного доступа, каждая из которых содержит соответствующие агенты безопасности и систему разделения доступа пользователя, соединенные с шиной управления и обмена данными соответствующего автоматизированного рабочего места пользователя или функционального сервера, систему защиты информации администратора от несанкционированного доступа, содержащую агент-администратор безопасности и систему разделения доступа администратора безопасности, соединенные с шиной управления и обмена данными соответствующего автоматизированного рабочего места администратора безопасности информации, а также сервер безопасности и базу данных безопасности, подключенные к шине управления и обмена данными сервера-контроллера домена, при этом автоматизированные рабочие места и функциональные серверы, сервер-контроллер домена и автоматизированное рабочее место администратора безопасности информации содержат установленные на них аппаратно-программные модули доверенной загрузки, устройства криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства криптографической защиты информации, передаваемой по протоколу IP подключены к шинам управления и обмена данными соответствующих автоматизированных рабочих мест и функциональных серверов, сервер контроллера домена и автоматизированного рабочего места администратора безопасности, все устройства криптографической защиты информации, передаваемой по локальной вычислительной сети по протоколу Ethernet, и устройства защиты информации, передаваемой по протоколу IP, соединены друг с другом по сетевой магистрали, причем по крайней мере одно автоматизированное рабочее место содержит установленные на

него и подключенные к его шине управления и обмена данными аппаратно-программный модуль доверенной загрузки, осуществляющий шифрование носителей информации, подключаемых по интерфейсу USB, и аппаратно-программный модуль доверенной загрузки, вырабатывающий и проверяющий электронную цифровую подпись, автоматизированные рабочие места пользователей и в автоматизированные рабочие места администраторов безопасности информации содержат средства усиленной аутентификации, которые подключены соответственно к шинам управления и обмена данными автоматизированных рабочих мест и к шинам управления и обмена данными автоматизированных рабочих мест администраторов безопасности информации, а каждая система защиты информации пользователя от несанкционированного доступа и система защиты информации администратора от несанкционированного доступа содержат соответствующую базу данных средств усиленной аутентификации пользователя и базу данных средств усиленной аутентификации администратора безопасности, соединенные соответственно с шиной управления и обмена данными соответствующего автоматизированного рабочего места пользователя или функционального сервера и с шиной управления и обмена данными автоматизированного рабочего места администратора безопасности информации, при этом сетевая магистраль имеет, по крайней мере, один разрыв, с каждой стороны которого включено по одному средству криптографической защиты информации, передаваемой по открытым каналам связи через неконтролируемую территорию, отличающаяся тем, что в автоматизированные рабочие места пользователей и в функциональные сервера дополнительно введены системы обмена с внешними системами защиты информации, которые подключены соответственно к шинам управления и обмена данными автоматизированных рабочих мест и к шинам управления и обмена данными функциональных серверов, причем в каждую систему защиты информации пользователя от несанкционированного доступа и в систему защиты информации функциональных серверов от несанкционированного доступа дополнительно введены соответствующие базы данных системы обмена с внешними системами защиты информации, соединенные соответственно с шиной управления и обмена данными соответствующего автоматизированного рабочего места пользователя или функционального сервера.