Приложение
к решению Федеральной службы по
интеллектуальной
собственности

ЗАКЛЮЧЕНИЕ
коллегии
по результатам рассмотрения ☒ возражения ☐ заявления

Коллегия в порядке, установленном пунктом 3 статьи 1248 Гражданского кодекса Российской Федерации (далее – Кодекс) и Правилами подачи возражений и заявлений и их рассмотрения в Палате по патентным спорам, утвержденными приказом Роспатента от 22.04.2003 № 56, зарегистрированным в Министерстве юстиции Российской Федерации 08.05.2003 № 4520 (далее – Правила ППС), рассмотрела возражение ЗАО "Лаборатория Касперского" (далее – заявитель), поступившее в 20.02.2015, на решение от 04.12.2014 Федеральной службы по интеллектуальной собственности (далее – Роспатент) об отказе в выдаче патента на изобретение по заявке № 2013119284/08, при этом установлено следующее.

Заявлена группа изобретений "Система и способ автоматического развертывания системы шифрования для пользователей, ранее работавших на ПК", совокупности признаков которых изложены в формуле, представленной в корреспонденции, поступившей 17.10.2014, в следующей редакции:

"1. Система применения политик шифрования данных, содержащая:

a. сервер администрирования, предназначенный для задания политик шифрования данных на, по крайней мере, одном компьютере;

b. упомянутый, по крайней мере, один компьютер, содержащий:

i. средство защиты, связанное с сервером администрирования, предназначенное для:

- получения политик шифрования данных от сервера

администрирования;

- определения учетной записи, по крайней мере, одного пользователя упомянутого компьютера;

- применения политик шифрования данных для, по крайней мере, одной учетной записи;

ii. средство шифрования, связанное со средством защиты, предназначенное для шифрования/расшифровки данных с помощью ключей шифрования в соответствии с упомянутыми политиками шифрования.

2. Система по п. 1, в которой средство защиты дополнительно предназначено для: создания ключей шифрования; обмена ключами шифрования между компьютером и сервером администрирования.

3. Система по п. 1, которая дополнительно содержит сервис ключей, связанный с сервером администрирования и предназначенный для создания ключей шифрования; обмена ключами шифрования с компьютером.

4. Система по п. 1, в которой средство защиты дополнительно служит для автоматического создания пароля учетной записи предзагрузки.

5. Способ применения политик шифрования данных, в котором:

a. получают политики шифрования данных, которые включают по крайней мере, опцию шифровать/не шифровать определенный набор данных с помощью ключей шифрования;

b. определяют список учетных записей пользователей упомянутого компьютера;

c. применяют упомянутые политики шифрования данных для, по крайней мере, одного пользователя из упомянутого списка учетных записей пользователей.

6. Способ по п. 5, в котором создают ключи шифрования данных с помощью средства защиты.

7. Способ по п. 6, в котором с помощью средства защиты передают

созданные ключи шифрования серверу администрирования.

8. Способ по п. 5, в котором создают ключи шифрования данных с помощью сервиса ключей.

9. Способ по п. 8, в котором с помощью сервиса ключей передают созданные ключи шифрования средству защиты.

10. Способ по п. 5, в котором в операционной системе семейства Windows, по крайней мере, одну учетную запись пользователя определяют с помощью ветки реестра HKEY_USERS.

11. Способ по п. 5, в котором список учетных записей пользователей определяют с помощью пользовательских каталогов на упомянутом компьютере.

12. Способ по п. 5, в котором список учетных записей пользователей определяют с помощью еще незагруженных веток реестра.

13. Способ по п. 5, в котором в операционной системе семейства UNIX учетные записи пользователей определяют по содержимому файла /etc/passwd.

14. Способ по п. 5, в котором данные являются данными одного или более жестких дисков.

15. Способ по п. 14, в котором полученные политики шифрования данных дополнительно включают, по крайней мере, одну из следующих опций: шифровать/расшифровать один или более жестких дисков с помощью ключей шифрования; автоматическое создание учетных записей для предзагрузки; критерии автоматического создания учетных записей для предзагрузки.

16. Способ по пп. 5, 15, в котором на шаге Ь. определяют список учетных записей пользователей компьютера в соответствии с упомянутыми критериями автоматического создания учетных записей для предзагрузки.

17. Способ по п. 16, в котором дополнительно создают учетные записи для предзагрузки для определенного списка учетных записей

пользователей компьютера.

18. Способ по п. 17, в котором дополнительно применяют упомянутые политики шифрования данных для созданных учетных записей для предзагрузки.

19. Способ по п. 16, в котором учетная запись предзагрузки содержит, по крайней мере, один из следующих параметров: имя, пароль, уникальный идентификатор пользователя, описание, дата и время создания, права доступа, флаг смены упомянутого пароля при следующем входе в операционную систему упомянутого компьютера.

20. Способ по п. 19, в котором пароль учетной записи предзагрузки задают автоматически.

21. Способ по п. 20, в котором выставляют флаг смены пароля упомянутой учетной записи предзагрузки при следующем входе в операционную систему упомянутого компьютера.

22. Способ по п. 19, в котором пароль учетной записи предзагрузки задает активный пользователь упомянутого компьютера.

23. Способ по п. 15, в котором критерии автоматического создания учетных записей предзагрузки содержат создание учетной записи предзагрузки для, по крайней мере, одного из следующих:

a. для всех существующих учетных записей на компьютере пользователей;

b. для всех существующих учетных записей на компьютере пользователей, соответствующих учетным записям пользователей из текущего домена или доменов, у которых есть доверительные отношения с текущим доменом;

c. для всех существующих учетных записей на компьютере пользователей, соответствующих учетным записям пользователей из доменов, у которых есть доверительные отношения с текущим доменом;

d. для всех локальных пользователей;

e. для встроенной локальной учетной записи администратора;

f. для владельца компьютера;

g. для текущего активного пользователя.

24. Способ по п. 23, в котором критерии автоматического создания учетных записей предзагрузки дополнительно содержат создание учетной записи предзагрузки для упомянутых на этапах a.-c.учетных записей, с использованием которых был выполнен вход в операционную систему компьютера в течение заранее определенного промежутка времени.

25. Способ по п. 5, в котором данные являются файлами и каталогами.

26. Способ по п. 25, в котором упомянутые политики шифрования данных создают автоматически для разных типов учетных записей.

27. Способ по п. 26, в котором для различных групп пользователей определяют различные наборы файлов и каталогов для шифрования.

28. Способ по п. 25, в котором упомянутые политики шифрования данных задает администратор центра защиты.

29. Способ по п. 25, в котором для, по крайней мере, одной определенной группы пользователей назначают политики шифрования данных, согласно которым каждый из пользователей упомянутой группы пользователей имеет доступ к зашифрованным файлам и каталогам, по крайней мере, одного другого пользователя из упомянутой группы пользователей."

Данная формула изобретения была принята к рассмотрению при экспертизе заявки по существу.

По результатам рассмотрения Роспатент 04.12.2014 принял решение об отказе в выдаче патента из-за несоответствия заявленной группы изобретений условию патентоспособности "изобретательский уровень".

В подтверждение данного вывода в решении Роспатента приведены сведения о следующих источниках информации:

− патентный документ US 2006/0242685 A1, опубл. 26.10.2006 (далее

– [1]);

− патентный документ US 2010/0241668 A1, опубл. 23.09.2010 (далее – [2]).

На решение об отказе в выдаче патента на изобретение в соответствии с пунктом 3 статьи 1387 Кодекса поступило возражение, в котором заявитель выразил несогласие с мотивировкой данного решения, указывая, что в решениях по патентным документам [1] и [2] "… нет упоминаний об использовании шифрования всего диска и политик шифрования дисков ... а также об автоматическом создании учетных записей для предзагрузки и критериях автоматического создания учетных записей для предзагрузки".

Изучив материалы дела, коллегия установила следующее.

С учетом даты подачи заявки (26.04.2013) правовая база для оценки патентоспособности заявленной группы изобретений включает Кодекс, Административный регламент исполнения Федеральной службой по интеллектуальной собственности, патентам и товарным знакам государственной функции по организации приема заявок на изобретение и их рассмотрения, экспертизы и выдачи в установленном порядке патентов Российской Федерации на изобретение, утвержденный приказом Министерства образования и науки Российской Федерации от 29 октября 2008г. № 327 и зарегистрированный в Минюсте РФ 20 февраля 2009г., рег. № 13413 (далее – Регламент).

В соответствии с пунктом 1 статьи 1350 Кодекса изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо.

В соответствии с пунктом 2 статьи 1350 Кодекса изобретение имеет изобретательский уровень, если для специалиста оно явным образом не следует из уровня техники. Уровень техники включает любые сведения, ставшие общедоступными в мире до даты приоритета изобретения.

В соответствии с пунктом 10.7.4.2 Регламента в качестве аналога

изобретения указывается средство того же назначения, известное из сведений, ставших общедоступными до даты приоритета изобретения.

В соответствии с подпунктом (1) пункта 24.5.3 Регламента изобретение явным образом следует из уровня техники, если оно может быть признано созданным путем объединения, изменения или совместного использования сведений, содержащихся в уровне техники, и/или общих знаний специалиста.

В соответствии с подпунктом (2) пункта 24.5.3 Регламента проверка изобретательского уровня может быть выполнена по следующей схеме:

определение наиболее близкого аналога в соответствии с пунктом 10.7.4.2 Регламента;

выявление признаков, которыми заявленное изобретение, охарактеризованное в независимом пункте формулы, отличается от наиболее близкого аналога (отличительных признаков);

выявление из уровня техники решений, имеющих признаки, совпадающие с отличительными признаками рассматриваемого изобретения;

анализ уровня техники с целью подтверждения известности влияния признаков, совпадающих с отличительными признаками заявленного изобретения, на указанный заявителем технический результат.

В соответствии с подпунктом (3) пункта 24.5.3 Регламента не признаются соответствующими условию изобретательского уровня изобретения, основанные, в частности, на дополнении известного средства какой-либо известной частью, присоединяемой к нему по известным правилам, если подтверждена известность влияния такого дополнения на достигаемый технический результат.

Существо заявленной группы изобретений выражено в приведенной выше формуле, которую коллегия принимает к рассмотрению.

Анализ доводов возражения и доводов, содержащихся в решении об

отказе в выдаче патента, касающихся оценки соответствия заявленного изобретения по независимому пункту 1 формулы условию патентоспособности "изобретательский уровень", показал следующее.

Из патентного документа [1] известна система применения политик шифрования данных ("система и способ для распределения политик безопасности для мобильных устройств" (реферат патентного документа [1]); "политика используется программным обеспечением агента в мобильном устройстве" (абзац [0032] патентного документа [1])). Известное решение по патентному документу [1] характеризуется следующими признаками:

сервер администрирования, предназначенный для задания политик шифрования данных на, по крайней мере, одном компьютере ("распределение политики безопасности информации мобильному компьютерному устройству" (абзац [0013] патентного документа [1]); "Система включает сервер ... сервер объединяется с существующими системами управления политиками безопасности и позволяет администраторам централизованно создавать новую мобильную политику безопасности ... и распределять эту политику безопасности мобильным устройствам" (абзац [0027] патентного документа [1])); наличием, по крайней мере, одного компьютера, содержащего средство защиты, связанное с сервером администрирования, предназначенное для получения политик шифрования данных от сервера администрирования ("модуль клиентского устройства используется, чтобы обеспечить безопасное функционирование и также упоминается как щит" (абзац [0027] патентного документа [1]); "Функция привратника заключается в получении пакетов политики от сервера и установки пакетов на целевые мобильные устройства" (абзац [0031] патентного документа [1]); "Административные инструменты на сервере позволяют автоматически сформировать пакеты политики и распределить на каждое мобильное устройство" (абзац [0033]

патентного документа [1])); наличием средства шифрования, связанного со средством защиты и предназначенного для шифрования/расшифровки данных с помощью ключей шифрования в соответствии с упомянутыми политиками шифрования ("Политики используются программным агентом на мобильном устройстве для шифрования данных" (абзац [0032] патентного документа [1]); "Модуль шифрования расшифровывает данные" (абзац [0065] патентного документа [1])).

Изобретение по независимому пункту 1 заявленной формулы отличается от известного из патентного документа [1] решения тем, что средство защиты предназначено для определения учетной записи, по крайней мере, одного пользователя упомянутого компьютера и применения политик шифрования данных для, по крайней мере, одной учетной записи.

Из патентного документа [2] известно решение, содержащее средства для определения учетной записи, по крайней мере, одного пользователя упомянутого компьютера ("различные типы учетных записей аккаунтов пользователя домена могут быть определены для различных типов пользователей" (абзац [0061] патентного документа [2])) и для применения политик шифрования данных для, по крайней мере, одной учетной записи ("база данных управления безопасностью может содержать пароли, ключи шифрования или друге учетные данные для каждого пользователя клиентского устройства ... такие учетные данные могут быть сохранены с использованием хэш или другой технологии" (абзац [0036] патентного документа [2])).

Необходимо подчеркнуть, что согласно материалам заявки технический результат, заключающийся в повышении уровня защиты информации от неавторизованного доступа, достигается за счет автоматического применения политик шифрования данных к устройствам конечных пользователей (см. описание с. 3). При этом в независимом пункте 1 приведенной выше формулы отсутствуют признаки,

характеризующие автоматическое применение политик шифрования данных к устройствам конечных пользователей. В связи с чем, совокупность признаков независимого пункта 1 формулы недостаточна для достижения указанного выше технического результат (подпункт (2) пункта 24.4. Регламента). Следовательно, подтверждения известности влияния отличительных признаков на технический результат не требуется (подпункт (7) пункта 24.5.3 Регламента).

Что касается доводов, изложенных в возражении, о том, что в патентном документе [1] и патентном документе [2] нет сведений об использовании шифрования всего диска и политик шифрования дисков, об автоматическом создании учетных записей для предзагрузки и критериях автоматического создания учетных записей для предзагрузки, необходимо отметить следующее.

В независимом пункте 1 приведенной выше формулы, в отношении которой было принято решение об отказе в выдаче патента, отсутствуют признаки, характеризующие использование шифрования всего диска и политик шифрования дисков, автоматическое создание учетных записей для предзагрузки и критерии автоматического создания учетных записей для предзагрузки.

Следовательно, можно сделать вывод о том, что заявленное изобретение по независимому пункту 1 формулы не соответствует условию патентоспособности "изобретательский уровень".

Анализ доводов возражения и доводов, содержащихся в решении об отказе в выдаче патента, касающихся оценки соответствия заявленного изобретения по независимому пункту 5 формулы условию патентоспособности "изобретательский уровень", показал следующее.

Из патентного документа [1] известен способ применения политик шифрования данных ("система и способ для распределения политик безопасности для мобильных устройств" (реферат патентного документа

[1]); "политика используется программным обеспечением агента в мобильном устройстве" (абзац [0032] патентного документа [1])). Известный способ по патентному документу [1] характеризуется следующими признаками:

получают политики шифрования данных ("модуль клиентского устройства используется, чтобы обеспечить безопасное функционирование и также упоминается как щит" (абзац [0027] патентного документа [1]); "Функция привратника заключается в получении пакетов политики от сервера и установки пакетов на целевые мобильные устройства" (абзац [0031] патентного документа [1]); "Административные инструменты на сервере позволяют автоматически сформировать пакеты политики и распределить на каждое мобильное устройство" (абзац [0033] патентного документа [1])), которые включают по крайней мере, опцию шифровать/не шифровать определенный набор данных с помощью ключей шифрования ("Политики используются программным агентом на мобильном устройстве для шифрования данных" (абзац [0032] патентного документа [1]); "Пара ключей, соответствующая контрольным журналам на отдельном мобильном устройстве, создается и управляется сервером" (абзац [0059] патентного документа [1]); "Модуль шифрования расшифровывает данные" (абзац [0065] патентного документа [1])).

Изобретение по независимому пункту 5 формулы отличается от известного из патентного документа [1] решения тем, что определяют список учетных записей пользователей упомянутого компьютера и применяют упомянутые политики шифрования данных для, по крайней мере, одного пользователя из упомянутого списка учетных записей пользователей.

Из патентного документа [2] известно решение, содержащее средства для определения списка учетных записей пользователей упомянутого компьютера ("различные типы учетных записей аккаунтов пользователя

домена могут быть определены для различных типов пользователей" (абзац [0061] патентного документа [2])) и для применения политик шифрования данных для, по крайней мере, одного пользователя из упомянутого списка учетных записей пользователей ("база данных управления безопасностью может содержать пароли, ключи шифрования или друге учетные данные для каждого пользователя клиентского устройства ... такие учетные данные могут быть сохранены с использованием хэш или другой технологии" (абзац [0036] патентного документа [2])).

Как отмечено выше, согласно описанию заявки технический результат достигается за счет автоматического применения политик шифрования данных к устройствам конечных пользователей. При этом в независимом пункте 5 приведенной выше формулы отсутствуют признаки, характеризующие автоматическое применение политик шифрования данных к устройствам конечных пользователей. В связи с чем, совокупность признаков независимого пункта 5 формулы недостаточна для достижения технического результат (подпункт (2) пункта 24.4. Регламента). Следовательно, подтверждения известности влияния отличительных признаков на технический результат не требуется (подпункт (7) пункта 24.5.3 Регламента).

Что касается доводов, изложенных в возражении, о том, что в патентном документе [1] и патентном документе [2] нет сведений об использовании шифрования всего диска и политик шифрования дисков, об автоматическом создании учетных записей для предзагрузки и критериях автоматического создания учетных записей для предзагрузки, необходимо отметить следующее.

В независимом пункте 5 приведенной выше формулы, в отношении которой было принято решение об отказе в выдаче патента, отсутствуют признаки, характеризующие использование шифрования всего диска и политик шифрования дисков, автоматическое создание учетных записей

для предзагрузки и критерии автоматического создания учетных записей для предзагрузки.

Следовательно, можно сделать вывод о том, что заявленное изобретение по независимому пункту 5 формулы не соответствует условию патентоспособности "изобретательский уровень".

На заседании коллегии 22.12.2015 от заявителя поступило ходатайство о переносе заседания коллегии с целью корректировки формулы изобретения. Ходатайство было удовлетворено (см. пункт 4.9 Правил ППС).

Скорректированная формула была представлена на заседании коллегии 11.04.2016, в следующей редакции:

"1. Система применения политик шифрования данных, содержащая:

а) сервер администрирования, предназначенный для задания политик шифрования данных на по крайней мере одном компьютере, при этом упомянутые данные являются данными одного или более жестких дисков, а политики шифрования данных включают, по крайней мере, одну из следующих опций:

• шифровать/расшифровать один или более жестких дисков с помощью ключей шифрования;

• автоматическое создание учетных записей PBA (англ. pre-boot authentication);

• критерий автоматического создания учетных записей PBA, при этом упомянутыми критериями являются:

i. для всех существующих учетных записей на упомянутом компьютере пользователей;

ii. для всех существующих учетных записей на компьютере пользователей, соответствующих учетным записям пользователей из доменов, у которых есть доверительные отношения с текущим доменом;

iii. для всех локальных пользователей;

iv. для встроенной локальной учетной записи администратора;

v. для владельца компьютера;

vi. для текущего активного пользователя;

vii. для учетных записей, определенных в упомянутых критериях i. - iii., с использованием которых был выполнен вход в операционную систему компьютера в течение заранее определенного промежутка времени;

б) упомянутый по крайней мере один компьютер, содержащий:

i. средство защиты, связанное с сервером администрирования и предназначенное для:

• получения политик шифрования данных от сервера администрирования;

• определения списка учетных записей пользователей в операционной системе (ОС), для которых необходимо создать учетные записи РВА в соответствии с полученными в политике критериями автоматического создания учетных записей РВА, при этом:

- если на жестком диске компьютера установлена ОС семейства Windows, упомянутое средство защиты анализирует ветку реестра HKEY_USERS, содержащую список всех загруженных профилей пользователей компьютера;

- если на компьютере установлена UNIX-подобная ОС, упомянутое средство защиты производит поиск учетных записей пользователей в файле /etc/passwd;

• создания учетных записей РВА для каждой обнаруженной учетной записи пользователя;

• создания ключей шифрования;

• передачи средству шифрования списка учетных записей, ключей шифрования и политик шифрования;

ii. средство шифрования, связанное со средством зашиты, предназначенное для шифрования/расшифровки данных с помощью ключей

шифрования в соответствии с упомянутыми политиками шифрования.

2. Система по п. 1, в которой учетные записи PBA содержат по меньшей мере следующие параметры:

• имя учетной записи пользователя в ОС;

• имя в PBA;

• пароль для аутентификации на этапе предзагрузки,

3. Система по п. 2, в которой параметры учетной записи PBA дополнительно содержат по меньшей мере одно из следующих полей:

• уникальный идентификатор пользователя (англ. SID – secure identifier);

• описание, дату и время создания упомянутой учетной записи PBA;

• дату и время изменения пароля упомянутой учетной записи PBA;

• права доступа;

• флаг необходимости смены пароля упомянутой учетной записи PBA при следующем входе в операционную систему.

4. Способ применения политик шифрования данных, в котором:

а) задают с помощью сервера администрирования политики шифрования данных на по крайней мере одном компьютере, при этом упомянутые данные являются данными одного или более жестких дисков, а политики шифрования данных включают, по крайней мере, одну из следующих опций:

• шифровать/расшифровать один или более жестких дисков с помощью ключей шифрования;

• автоматическое создание учетных записей PBA (англ. pre-boot authentication);

• критерии автоматического создания учетных записей PBA, при этом упомянутыми критериями являются:

i. для всех существующих учетных записей на упомянутом компьютере пользователей;

ii. для всех существующих учетных записей на компьютере пользователей, соответствующих учетным записям пользователей из доменов, у которых есть доверительные отношения с текущим доменом;

iii. для всех локальных пользователей;

iv. для встроенной локальной учетной записи администратора;

v. для владельца компьютера;

vi. для текущего активного пользователя;

vii. для учетных записей, определенных в упомянутых критериях i. - iii., с использованием которых был выполнен вход в операционную систему компьютера в течение заранее определенного промежутка времени;

б) получают с помощью средства защиты на компьютере от сервера администрирования политики шифрования данных;

в) определяют с помощью средства защиты список учетных записей пользователей в операционной системе (ОС), для которых необходимо создать учетные записи PBA в соответствии с полученными в политике критериями автоматического создания учетных записей PBA, при этом:

- если на жестком диске компьютера установлена ОС семейства Windows, упомянутое средство защиты анализирует ветку реестра HKEY_USERS, содержащую список всех загруженных профилей пользователей компьютера;

- если на компьютере установлена UNIX-подобная ОС, упомянутое средство защиты производит поиск учетных записей пользователей в файле /etc/passwd;

г) создают с помощью средства защиты учетные записи PBA для каждой обнаруженной учетной записи пользователя;

д) создают с помощью средства защиты ключи шифрования;

е) с помощью средства зашиты передают средству шифрования список учетных записей, ключи шифрования и политики шифрования;

ж) выполняют с помощью средства шифрования

шифрование/расшифровку данных с помощью ключей шифрования в соответствии с упомянутыми политиками шифрования.

5. Способ по п. 4, в котором список учетных записей пользователей определяют с помощью пользовательских каталогов на упомянутом компьютере.

6. Способ по п. 4, в котором учетные записи PBA содержат по меньшей мере следующие параметры:

• имя учетной записи пользователя в ОС;

• имя учетной записи PBA;

• пароль для аутентификации на этапе предзагрузки.

7. Способ по п. 6, в котором параметры учетной записи PBA дополнительно содержат по крайней мере одно из следующих полей:

• уникальный идентификатор пользователя (англ. SID - secure identifier);

• описание, дату и время создания упомянутой учетной записи PBA;

• дату и время изменения пароля упомянутой учетной записи PBA;

• права доступа;

• флаг необходимости смены пароля упомянутых учетных записей PBA при следующем входе в операционную систему.

8. Способ по п. 7, в котором пароль учетной закиси PBA задают автоматически."

Данная скорректированная формула была принята коллегией к рассмотрению.

На основании пункта 5.1 Правил ППС, материалы заявки были направлены для проведения дополнительного информационного поиска.

По результатам проведения дополнительного поиска 12.06.2016 были представлены: отчет о дополнительном информационном поиске и экспертное заключение, в котором сделан вывод о патентоспособности заявленного изобретения.

В отчете о дополнительном поиске приведены следующие источники информации:

− [1];

− патентный документ US 2012/0179915 A1, 12.07.2012 (далее − [3]);

− патентный документ US 2010/0303240 A1, 02.12.2010 (далее − [4]);

− патентный документ US 2009/0319806 A1, 24.12.2009 (далее − [5]);

− патентный документ RU 2009107223 A, 10.09.2010 (далее − [6]).

При этом, в экспертном заключении было отмечено следующее.

В независимых пунктах 1 и 4 скорректированной формулы изобретения, представленной на заседании коллегии 11.04.2016, указаны признаки "политики шифрования данных включают, по крайней мере, одну из следующих опций: шифровать/расшифровать один или более жестких дисков с помощью ключей шифрования; автоматическое создание учетных записей PBA (англ. pre-boot authentication); критерий автоматического создания учетных записей PBA", выраженные в виде альтернативы. При этом во всех альтернативных вариантах выполнения изобретений по независимым пунктам 1 и 4, кроме альтернативного варианта по независимым пунктам 1 и 4, в котором политики шифрования данных включают опции шифровать/расшифровать один или более жестких дисков с помощью ключей шифрования; автоматическое создание учетных записей PBA (англ. pre-boot authentication); критерий автоматического создания учетных записей PBA, не будут реализованы назначения заявленных системы и способа, а именно применение политик шифрования данных.

Кроме того, в экспертном заключении было указано, что приведенный в независимых пункта 1 и 4 скорректированной формулы, характеризующей группу изобретений, признак "передают средству шифрования список учетных записей" не ясен.

Вышеуказанные материалы, представленные по результатам проведения дополнительного поиска, были направлены в адрес заявителя.

На заседании коллегии 24.08.2016 от заявителя поступило ходатайство о корректировке формулы путем исключения из независимых пунктов 1 и 4 альтернативных вариантов изобретений и признака, вызвавших замечания экспертизы, с приложением скорректированной формулы. Данные изменения не требуют проведения дополнительного информационного поиска.

Таким образом, коллегией не выявлено каких-либо обстоятельств, препятствующих признанию группы изобретений, охарактеризованной скорректированной формулой, представленной на заседании коллегии 24.08.2016, соответствующим условиям патентоспособности.

Учитывая вышеизложенное, коллегия пришла к выводу о наличии оснований для принятия Роспатентом следующего решения:

удовлетворить возражение, поступившее 20.02.2015, отменить решение Роспатента от 04.12.2014, выдать патент Российской Федерации на изобретение с формулой, представленной на заседании коллегии 24.08.2016.

(21)2013119284/08

(51) МПК

G06F 21/00 (2013.01)

G06F 15/16 (2006.01)

(57) “1. Система применения политик шифрования данных, содержащая:

а) сервер администрирования, предназначенный для задания политик шифрования данных на по крайней мере одном компьютере, при этом упомянутые данные являются данными одного или более жестких дисков, а политики шифрования данных включают опции:

• шифровать/расшифровать один или бо алее жестких дисков с помощью ключей шифрования;

• автоматическое создание учетных записей PBA (англ. pre-boot authentication);

• критерии автоматического создания учетных записей PBA, при этом упомянутыми критериями являются:

i. для всех существующих учетных записей на упомянутом компьютере пользователей;

ii. для всех существующих учетных записей на компьютере пользователей, соответствующих учетным записям пользователей из доменов, у которых есть доверительные отношения с текущим доменом;

iii. для всех локальных пользователей;

iv. для встроенной локальной учетной записи администратора;

v. для владельца компьютера;

vi. для текущего активного пользователя;

vii. для учетных записей, определенных в упомянутых критериях i. - iii., с

использованием которых был выполнен вход в операционную систему компьютера в течение заранее определенного промежутка времени;

б) упомянутый по крайней мере один компьютер, содержащий:

i. средство защиты, связанное с сервером администрирования и предназначенное для:

• получения политик шифрования данных от сервера администрирования;

• определения списка учетных записей пользователей в операционной системе (ОС), для которых необходимо создать учетные записи РВА в соответствии с полученными в политике критериями автоматического создания учетных записей РВА, при этом:

- если на жестком диске компьютера установлена ОС семейства Windows, упомянутое средство защиты анализирует ветку реестра HKEY_USERS, содержащую список всех загруженных профилей пользователей компьютера;

- если на компьютере установлена UNIX-подобная ОС, упомянутое средство защиты производит поиск учетных записей пользователей в файле /etc/passwd;

• создания учетных записей РВА для каждой обнаруженной учетной записи пользователя;

• создания ключей шифрования;

• передачи средству шифрования ключей шифрования и политик шифрования;

ii. средство шифрования, связанное со средством зашиты, предназначенное для шифрования/расшифровки данных с помощью ключей шифрования в соответствии с упомянутыми политиками шифрования.

2. Система по п. 1, в которой учетные записи РВА содержат по меньшей мере следующие параметры:

• имя учетной записи пользователя в ОС;

• имя в PBA;

• пароль для аутентификации на этапе предзагрузки,

3. Система по п. 2, в которой параметры учетной записи PBA дополнительно содержат по меньшей мере одно из следующих полей:

• уникальный идентификатор пользователя (англ. SID – secure identifier);

• описание, дату и время создания упомянутой учетной записи PBA;

• дату и время изменения пароля упомянутой учетной записи PBA;

• права доступа;

• флаг необходимости смены пароля упомянутой учетной записи PBA при следующем входе в операционную систему.

4. Способ применения политик шифрования данных, в котором:

а) задают с помощью сервера администрирования политики шифрования данных на по крайней мере одном компьютере, при этом упомянутые данные являются данными одного или более жестких дисков, а политики шифрования данных включают опции:

• шифровать/расшифровать один или более жестких дисков с помощью ключей шифрования;

• автоматическое создание учетных записей PBA (англ. pre-boot authentication);

• критерии автоматического создания учетных записей PBA, при этом упомянутыми критериями являются:

i. для всех существующих учетных записей на упомянутом компьютере пользователей;

ii. для всех существующих учетных записей на компьютере пользователей, соответствующих учетным записям пользователей из доменов, у которых есть доверительные отношения с текущим доменом;

iii. для всех локальных пользователей;

iv. для встроенной локальной учетной записи администратора;

v. для владельца компьютера;

vi. для текущего активного пользователя;

vii. для учетных записей, определенных в упомянутых критериях i. - iii., с использованием которых был выполнен вход в операционную систему компьютера в течение заранее определенного промежутка времени;

б) получают с помощью средства защиты на компьютере от сервера администрирования политики шифрования данных;

в) определяют с помощью средства защиты список учетных записей пользователей в операционной системе (ОС), для которых необходимо создать учетные записи РВА в соответствии с полученными в политике критериями автоматического создания учетных записей РВА, при этом:

- если на жестком диске компьютера установлена ОС семейства Windows, упомянутое средство защиты анализирует ветку реестра HKEY_USERS, содержащую список всех загруженных профилей пользователей компьютера;

- если на компьютере установлена UNIX-подобная ОС, упомянутое средство защиты производит поиск учетных записей пользователей в файле /etc/passwd;

г) создают с помощью средства защиты учетные записи РВА для каждой обнаруженной учетной записи пользователя;

д) создают с помощью средства защиты ключи шифрования;

е) с помощью средства зашиты передают средству шифрования ключи шифрования и политики шифрования;

ж) выполняют с помощью средства шифрования шифрование/расшифровку данных с помощью ключей шифрования в соответствии с упомянутыми политиками шифрования.

5. Способ по п. 4, в котором список учетных записей пользователей определяют с помощью пользовательских каталогов на упомянутом компьютере.

6. Способ по п. 4, в котором учетные записи РВА содержат по меньшей мере следующие параметры:

• имя учетной записи пользователя в ОС;

• имя учетной записи РВА;

• пароль для аутентификации на этапе предзагрузки.

7. Способ по п. 6, в котором параметры учетной записи РВА дополнительно содержат по крайней мере одно из следующих полей:

• уникальный идентификатор пользователя (англ. SID - secure identifier);

• описание, дату и время создания упомянутой учетной записи РВА;

• дату и время изменения пароля упомянутой учетной записи РВА;

• права доступа;

• флаг необходимости смены пароля упомянутых учетных записей РВА при следующем входе в операционную систему.

8. Способ по п. 7, в котором пароль учетной закиси РВА задают автоматически.”

Приоритет:

26.04.2013

(56) US 2006/0242685 A1, 26.10.2006
US 2012/0179915 A1, 12.07.2012
US 2010/0303240 A1, 02.12.2010
US 2009/0319806 A1, 24.12.2009
RU 2009107223 A, 10.09.2010

Примечание: при публикации сведений о выдаче патента будет использовано первоначальное описание.