РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 658 894**(13) **C1**

(51) МПК
G06F 21/62 (2013.01)
G06F 21/45 (2013.01)
H04L 9/32 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/62 (2006.01); G06F 21/45 (2006.01); H04L 9/32 (2006.01)

(21)(22) Заявка: **2017126662, 26.07.2017**

(24) Дата начала отсчета срока действия патента:
26.07.2017

Дата регистрации:
25.06.2018

Приоритет(ы):
(22) Дата подачи заявки: **26.07.2017**

(45) Опубликовано: **25.06.2018** Бюл. № **18**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Иванова Елена Вадимовна (RU),
Копелев Михаил Александрович (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **US 8738531 B1, 27.05.2014. US 7587749 B2, 08.09.2009. RU 2391783 C2, 10.06.2010. RU 2439692 C2, 10.01.2012.**

(54) Способ управления доступом к данным с защитой учетных записей пользователей

(57) Реферат:

Изобретение относится к области информационной безопасности. Технический результат – обеспечение децентрализованного контроля над правами доступа к данным. Способ заключается в том, что со стороны администратора защищаемого объекта с данными объекта генерируют уникальный идентификатор ИД защищаемого объекта, генерируют случайный симметричный ключ КА администрирования объекта, получают симметричный ключ шифрования данных объекта КО путем вычисления производного ключа от ключа КА с использованием идентификатора ИД в качестве модификатора, зашифровывают данные защищаемого объекта на ключе КО, получая зашифрованные данные ШДО, формируют блок данных служебной информации, содержащий идентификатор ИД, сведения о защищаемом объекте и спецификацию использующихся криптографических функций, формируют список доступа к объекту, состоящий из учетных записей пользователей, которым предоставляется доступ к защищаемому объекту, причем по крайней мере одна из учетных записей принадлежит администратору объекта, выполняя для каждой учетной записи следующие действия: получают у выбранного пользователя, имеющего асимметричную пару ключей в составе открытого ключа и секретного ключа, его открытый ключ, генерируют случайное число, принимают его в качестве временного идентификатора, формируют идентификатор учетной записи, принимая в качестве его значения временный идентификатор, генерируют случайную асимметричную пару ключей в составе открытого ключа и секретного ключа, генерируют случайный симметричный ключ КЗ учетной записи, вычисляют общий симметричный ключ КЗП из секретного ключа и открытого ключа, зашифровывают ключ КЗ на ключе КЗП, получая зашифрованный ключ, принимают решение о наделении пользователя полномочиями администратора, формируют значение параметра, характеризующего наличие у пользователя полномочий администратора,

RU 2658894 C1

RU 2658894 C1

формируют блок данных, зашифровывают его на ключе КЗ, получая зашифрованные данные, формируют текстовое описание учетной записи выбранного пользователя, формируют блок проверочных данных администрирования, зашифровывают его на ключе КА, получая зашифрованные данные, формируют учетную запись выбранного пользователя, сохраняют совместно зашифрованные данные ШДО, служебную информацию, список доступа к объекту.

RU 2658894 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 658 894**(13) **C1**

(51) Int. Cl.
G06F 21/62 (2013.01)
G06F 21/45 (2013.01)
H04L 9/32 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/62 (2006.01); G06F 21/45 (2006.01); H04L 9/32 (2006.01)

(21)(22) Application: **2017126662, 26.07.2017**

(24) Effective date for property rights:
26.07.2017

Registration date:
25.06.2018

Priority:
(22) Date of filing: **26.07.2017**

(45) Date of publication: **25.06.2018** Bull. № **18**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Ivanova Elena Vadimovna (RU),
Kopelev Mikhail Aleksandrovich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2658894 C1

(54) METHOD OF THE DATA ACCESS CONTROL WITH THE USERS ACCOUNTS PROTECTION

(57) Abstract:

FIELD: information technologies.

SUBSTANCE: invention relates to information security. Method consists in that on the part of the protected object with the object data administrator, generating the protected object ID unique identifier, generating the object administration random symmetric key CA, obtaining the CO object data encryption symmetric key by the derived key calculation from the CA key using the ID identifier as the modifier, encrypting the protected object data on the CO key, receiving the encrypted SDO data, generating the service data block containing the ID identifier, information about the protected object and specification of the used cryptographic functions, forming the access to the object list, consisting of users accounts, to which access to the protected object is granted, wherein at least one of the accounts belongs to the object administrator, performing the following actions for each account: receiving, from the selected user having the asymmetric key pair including the public key and private key, its public key, generating the random number, taking it as the temporary identifier, generating the account identifier, taking the temporary identifier as its value, generating the random asymmetric keys pair including the public key and private key, generating the account random symmetric account key KZ, calculating the common symmetrical key KZP from the private key and the public key, encrypting the KZ key on the KZP key, receiving the encrypted key, deciding on the administrator rights assignment to the user, generating the parameter value, characterizing the administrator rights availability in the user, generating the data block, encrypting it on the KZ key, receiving the encrypted data, forming the selected user account text description, generating the administration verification data block, encrypting it on the CA key, receiving the encrypted data, generating the selected user account, storing together the SDO encrypted data, service information, the object access list.

EFFECT: enabling the decentralized control over the data access rights.

1 cl

RU 2658894 C1

Область техники, к которой относится изобретение

Предлагаемое изобретение относится к области информационной безопасности и криптографии и, в частности, к способам управления и контроля доступа к конфиденциальной информации, хранимой и обрабатываемой в автоматизированных компьютерных системах.

Уровень техники

При построении систем безопасности применяются разнообразные методы управления доступом (дискреционный, мандатный, ролевой и иные методы). Дискреционная модель управления доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации (Руководящий документ: Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. - М.: Государственная техническая комиссия России, 1992 г.).

Дискреционное управление доступом (discretionary access control, DAC) основывается на списках управления доступом или матрицах доступа защищаемых объектов (Access Control List, ACL), в которых перечисляются субъекты (пользователи или процессы), имеющие права доступа к данному объекту, и их полномочия.

В дискреционной модели доступа и по требованиям руководящих документов предусматривается разделение ролей пользователей, а именно, выделяется роль администратора, которому предоставляется исключительное право на формирование списка доступа и на которого возлагается обязанность по поддержанию этого списка в актуальном состоянии в соответствие с используемой Политикой безопасности.

В рамках дискреционной модели предусматривается иерархическое управление доступом и возможность делегирования прав администратора. Например, в большинстве операционных систем, таких как Unix или Windows, имеется главный администратор (или суперпользователь), который имеет право назначать администраторов отдельных объектов (владельцев объектов) и делегировать им права по управлению списками доступа этих объектов.

Для защиты информации традиционно используется шифрование. В результате, управление доступом к данным защищаемого объекта сводится к управлению доступа к секретному ключу шифрования этих данных. Без использования секретного ключа шифрования не обойтись и при удаленном доступе к данным по незащищенным каналам связи, например, при хранении информации в облачных сервисах.

В общем случае и управление другими полномочиями (внесение изменений в данные, исполнение кода и др.) может быть реализовано через управление доступом к определенным секретным параметрам (ключам). Например, легитимность вносимых изменений или кода перед исполнением может проверяться по контрольной сумме, вычисляемой с использованием секретного параметра.

Известен способ предоставления доступа к большому объему защищаемой информации многим пользователям (патент РФ №2391783, приоритет от 14.01.20015 г.), при котором информация вместо того, чтобы многократно зашифровываться на индивидуальных секретных ключах пользователей, зашифровывается один раз на технологическом ключе. Сам технологический ключ зашифровывается на индивидуальных ключах пользователей (или по цепочке на других технологических ключах, последний из которых зашифровывается на ключе конкретного пользователя) и в зашифрованном виде передается этим пользователям. В известном способе формирование, проверка и актуализация списков доступа не рассматривается и

возлагается на некоторый доверенный сервис, а самостоятельная смена параметров авторизации (открытых ключей) пользователей не предусмотрена.

При размещении данных и передачи управления доступа к ним недоверенной стороне (например, провайдеру облачных сервисов) наряду с шифрованием информации необходимо контролировать соблюдение прав доступа к данным на стороне пользователя. Удаленно отличить легитимного пользователя от злоумышленника можно только по наличию у него (обладанию им) секретного параметра (ключа). То есть, авторизация пользователя должна, в частности, состоять в том, что он с помощью своего секретного параметра вычисляет или находит ключ шифрования данных. В качестве такого секретного параметра авторизации могут выступать: пароль, непосредственно секретный ключ или индивидуальное устройство с секретным ключом (eToken), которое не дает считать сам ключ, но позволяет выполнить с использованием этого ключа некоторые преобразования.

При долговременном хранении и обработке защищаемой информации по соображениям безопасности и по требованиям руководящих документов необходимо иметь возможности сменить как ключ шифрования данных, так и индивидуальные параметры авторизации пользователей. Например, данные действия требуются при компрометации или угрозе компрометации одного из этих параметров.

При этом при большом числе пользователей непосредственное взаимодействие администратора объекта с каждым пользователем для изменений параметров его авторизации может быть технически сложно и/или неосуществимо за приемлемое время. Кроме того, ознакомление администратора с секретными параметрами авторизации пользователя может представлять угрозу безопасности: пользователь может использовать эти же параметры для доступа к другому защищаемому объекту, к которому у данного администратора доступа нет. Требование от пользователя применять уникальные параметры авторизации для каждого защищаемого объекта порождает уже проблемы у пользователей по управлению этими параметрами при большом числе объектов, к которым допущен этот пользователь.

Поэтому возможность для пользователя независимо от других пользователей и администраторов сменить свои параметры авторизации и возможность для администратора поменять ключ шифрования данных без участия пользователей является несомненным положительным свойством системы управления доступом.

С другой стороны, такие возможности пользователей по независимой смене параметров авторизации лишают администратора простого способа контролировать целостность списка доступа по контрольной сумме (в том числе, и по контрольной сумме с использованием ключа администрирования). Для злоумышленника же, наоборот, появляется перспектива сформировать учетную запись (или заменить учетную запись легитимного пользователя) с известными ему параметрами авторизации в надежде, что при смене администратором ключа шифрования эти параметры авторизации позволят вычислить новый ключ шифрования и, соответственно, получить доступ к защищаемой информации. Поэтому требуется отдельные средства проверки подлинности учетных записей пользователей в списках доступа.

При большом числе пользователей другим востребованным положительным свойством системы управления доступа является эффективный поиск своей учетной записи по параметрам авторизации, поскольку опробование всех учетных записей на предмет авторизации может потребовать неприемлемо большого времени.

Наиболее полное решение отмеченных проблем представлено в способе (патент США №8738531, приоритет от 08.07.2008 г.), который далее рассматривается в качестве

прототипа.

В прототипе предлагается в учетной записи пользователя размещать в зашифрованном на открытом ключе пользователя ОКП ключ шифрования данных объекта КО.

Системы шифрования с открытым ключом используют в криптографических операциях взаимосвязанные открытый ключ (ОК) и секретный ключ (СК), которые эффективно генерируются с помощью процедуры GenPub ()=(ОК, СК). Ключ ОК распространяется среди корреспондентов для зашифровывания сообщений С данному адресату с помощью процедуры PubEncrypt (С, ОК) = ШС. Пользователь (адресат) хранит в тайне ключ СК и использует его для расшифровывания присланных ему шифрованных сообщений ШС с помощью процедуры PubDecrypt (ШС, ШС) = С. Такая схема шифрования основывается на свойстве, что вычисление СК и/или нахождение С по известным ОК и ШС требует неприемлемых вычислительных ресурсов. Известны несколько систем шифрования с открытым ключом, из которых наибольшее распространение получила система RSA (Патент США №4405829, приоритет от 14.12.1977 г.).

В рассматриваемом прототипе учетная запись пользователя формируется администратором (владельцем) из значений:

- ОКП - открытого ключа пользователя;
- ШКО = PubEncrypt (КО, ОКП) - ключа шифрования объекта КО, зашифрованного на открытом ключе пользователя;
- СК = Hash (ОКП, КО) - контрольной суммы учетной записи, являющейся результатом хэширования открытого ключа пользователя и ключа защиты объекта.

Такая структура учетных записей позволяет пользователю эффективно находить свою учетную запись по открытому ключу ОКП и вычислять ключ защиты объекта КО = PubDecrypt (ШКО, СКП). Имея ключ защиты объекта КО, пользователь может, сгенерировав новую пару ОКП и СКП открытого и секретного ключей, вычислить без участия администратора учетную запись для новых ключей, т.е. сменить свои параметры авторизации/доступа к объекту самостоятельно. Администратор, как и любой из пользователей, может перешифровать объект на новом ключе КО и сформировать для нового ключа учетные записи пользователей по указанным открытым ключам ОКП без участия других пользователей. При этом контрольная сумма СК позволяет удостовериться, что используемый открытый ключ был заявлен лицом, обладающим ключом защиты объекта КО, т.е. легитимным пользователем, а не злоумышленником.

Основным недостатком прототипа является то, что в нем фактически отсутствует роль администратора: любой легитимный пользователь может выступить в качестве администратора и добавить новых пользователей (или заменить в учетной записи другого пользователя открытый ключ на известный ему), что администратор не может технически обнаружить. Это свойство влечет угрозу безопасности: перед увольнением злоумышленник мог создать несколько фиктивных учетных записей (или подменить открытые ключи в учетных записях пользователей, редко обращающихся к объекту и долгое время не обнаруживающих такой подмены), что позволит ему сохранить доступ к объекту после исключения своей учетной записи и смене ключа защиты объекта администратором.

Для противодействия этой угрозе в прототипе предложено формировать ключ шифрования данных объекта из 2-х ключей: из ключа защиты объекта КО и ключа сервера КС, для получения которого надо отдельно проходить авторизацию на доверенном сервисе. Необходимость использования дополнительного доверенного

сервиса авторизации фактически дезавуирует заявленную в прототипе структуру учетных записей: что улучшает прототип по сравнению с этой доверенной авторизацией становится неясно.

Другим недостатком прототипа является непосредственное перечисление в списке доступа отрытых ключей пользователей. В типичных ситуациях, когда пользователь использует одну и ту же пару отрытого и секретного ключа для доступа к разным защищаемым объектам, у злоумышленника появляется возможность проанализировать списки доступа и выделить открытые ключи, которые фигурируют наиболее часто. Сосредоточив усилия на вычислении соответствующих секретных ключей, злоумышленник в случае успеха получает доступ сразу к нескольким защищаемым объектам вместо того, чтобы затрачивать аналогичные вычислительные ресурсы для доступа к каждому из этих объектов по отдельности.

Кроме того, открытые ключи пользователей могут быть получены из публичных сертификатов ключей, что позволяет злоумышленнику выявить круг лиц, допущенных к тому или иному защищаемому объекту, и, тем самым, косвенно определить характер содержащихся в нем данных и более обоснованно выбрать объект атаки.

Раскрытие изобретения

Техническим результатом является обеспечение:

1) децентрализованного контроля над правами доступа путем предоставление доступа к информации по результатам локальной авторизации пользователей без использования доверенных централизованных сервисов авторизации;

2) дифференциации ролей пользователей путем выделение ролей администраторов с возможностью делегирования прав администратора другим пользователям;

3) независимой смены параметров авторизации пользователями и администраторами, при которой замена параметров авторизации не требует взаимодействия с остальными пользователями и администраторами;

4) эффективного поиска для пользователей своей учетной записи в списке доступа;

5) независимой сменой параметров защиты объекта, при которой замена администратором параметров защиты информации не требует взаимодействия с пользователями и другими администраторами;

6) выявления несанкционированных изменений в списке доступа;

7) сокрытия состава лиц, имеющих доступ к защищаемой информации.

Для этого предлагается способ управления доступом к данным в компьютере, причем компьютер имеет установленное программное средство, выполненное с возможностью

- генерировать уникальные идентификаторы,
- генерировать случайные числа,
- генерировать случайные симметричные ключи,
- генерировать случайные асимметричные пары ключей в составе открытого ключа и секретного ключа,
- вычислять значение функции хэширования,
- вычислять производный симметричный ключ из исходного симметричного ключа и значения модификатора,
- вычислять общий симметричный ключ из секретного ключа и открытого ключа,
- зашифровывать и расшифровывать данные на симметричном ключе,
- зашифровывать и расшифровывать симметричный ключ на симметричном ключе;

способ заключается в том, что, со стороны администратора защищаемого объекта с данными объекта ДО выполняют следующие действия:

- генерируют уникальный идентификатор ИД защищаемого объекта;

- генерируют случайный симметричный ключ КА администрирования объекта;
- получают симметричный ключ шифрования данных объекта КО путем вычисления производного ключа от ключа КА с использованием идентификатора ИД в качестве модификатора;
- зашифровывают данные защищаемого объекта ДО на ключе КО, получая зашифрованные данные ШДО;
- формируют блок данных служебной информации ДС, содержащий идентификатор ИД, сведения о защищаемом объекте и спецификацию использующихся криптографических функций СФ;
- формируют список доступа ДД к объекту, состоящий из учетных записей пользователей, которым предоставляется доступ к защищаемому объекту, причем по крайней мере одна из учетных записей принадлежит администратору объекта, выполняя для каждой учетной записи УЗ следующие действия:
  - получают у выбранного пользователя, имеющего асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, его открытый ключ ОКП;
  - генерируют случайное число, принимают его в качестве временного идентификатора ВИ;
  - формируют идентификатор ИЗ учетной записи УЗ, принимая в качестве его значения временный идентификатор ВИ;
  - генерируют случайную асимметричную пару ключей в составе открытого ключа ОКЗ и секретного ключа СКЗ;
  - генерируют случайный симметричный ключ КЗ учетной записи УЗ;
  - вычисляют общий симметричный ключ КЗП из секретного ключа СКЗ и открытого ключа ОКП;
  - зашифровывают ключ КЗ на ключе КЗП, получая зашифрованный ключ ШКЗ;
  - принимают решение о наделении пользователя полномочиями администратора;
  - формируют значение параметра ПА, характеризующего наличие у пользователя полномочий администратора;
  - формируют блок данных ДЗ из следующих данных:
    - ключ ОКП,
    - параметр ПА,
    - ключ КА, если параметр ПА указывает на наличие у пользователя полномочий администратора, иначе - ключ КО;
  - зашифровывают блок данных ДЗ на ключе КЗ, получая зашифрованные данные ШДЗ;
  - формируют текстовое описание Т учетной записи УЗ выбранного пользователя;
  - формируют блок проверочных данных администрирования ДА из следующих данных:
    - ключ КЗ,
    - параметр ПА,
    - текстовое описание Т;
  - зашифровывают блок данных ДА на ключе КА, получая зашифрованные данные ШДА;
  - формируют учетную запись выбранного пользователя УЗ в виде следующего блока данных:
    - идентификатор ИЗ,
    - ключ ОКЗ,
    - зашифрованный ключ ШКЗ,

- зашифрованные данные ШДЗ,
- зашифрованные данные ШДА;
- сохраняют совместно следующие данные:
  - зашифрованные данные ШДО,
  - служебную информацию ДС,
  - список доступа к объекту ДД;

при необходимости доступа к защищаемому объекту со стороны пользователя, имеющего асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, выполняют следующие действия:

- (А) извлекают из служебной информации ДС идентификатор объекта ИД и спецификацию использующихся криптографических функций СФ;
- вычисляют общий симметричный ключ КПП из секретного ключа СКП и открытого ключа ОКП;
- вычисляют значение функции хэширования от блока данных, составленного из идентификатора ИД и ключа КПП, получая постоянное значение идентификатора ИЗ;
- если доступ выполняется в первый раз с момента формирования администратором объекта списка доступа, то переходят к этапу (Б), иначе переходят к этапу (В);
- (Б) получают у администратора объекта временный идентификатор ВИ, назначенный учетной записи данного пользователя при первичном формировании списка доступа;
- находят в списке доступа ДД учетную запись, у которой значение идентификатора ИЗ совпадает с ВИ;
- заменяют в учетной записи пользователя значение идентификатора ИЗ на вычисленное постоянное значение;
- (В) находят в списке доступа ДД учетную запись, у которой значение ИЗ совпадает с вычисленным;
- получают из найденной учетной записи ключи ОКЗ, ШКЗ и зашифрованные данные ШДЗ, ШДА;
- вычисляют общий симметричный ключ КЗП из ключей СКП и ОКЗ;
- расшифровывают ключом КЗП зашифрованный ключ ШКЗ, получая секретный ключ КЗ;
- расшифровывают ключом КЗ зашифрованные данные ШДЗ, получая значение параметра ПА и ключ К;
- если параметр ПА указывает на наличие у пользователя полномочий администратора, принимают ключ К в качестве ключа администрирования КА и вычисляют для него производный ключ, используя идентификатор ИД в качестве модификатора, получая ключ шифрования данных КО;
- если параметр ПА указывает на отсутствие у пользователя полномочий администратора, принимают ключ К в качестве ключа шифрования данных КО;
- расшифровывают зашифрованные данные ШДО с помощью ключа КО, получая данные защищаемого объекта ДО;

при необходимости со стороны пользователя, имеющего асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, перейти на использование другой асимметричной пары ключей в составе открытого ключа ОКМ и секретного ключа СКМ и иметь доступ к защищаемому объекту, выполняют следующие действия:

- выполняют действия для доступа к защищаемому объекту согласно этапу А, получая идентификатор ИД, ключи ОКЗ, КЗ, К и значение параметра ПА;
- вычисляют общий симметричный ключ КММ из секретного ключа СКМ и

открытого ключа ОКМ;

- вычисляют значение функции хэширования от блока данных, составленного из идентификатора ИД и ключа КММ, получая модифицированное постоянное значение идентификатора ИЗ;
- заменяют в учетной записи пользователя УЗ значение идентификатора ИЗ на модифицированное значение;
- вычисляют модифицированное значение ключа КЗП как общий симметричный ключ для ключей СКМ и ОКЗ;
- зашифровывают ключ КЗ на модифицированном ключе КЗП, получая модифицированное значение зашифрованного ключ ШКЗ;
- заменяют в учетной записи пользователя УЗ значение зашифрованного ключа ШКЗ на модифицированное значение;
- формируют модифицированный блок данных ДЗ из следующих данных:
  - ключ ОКМ,
  - параметр ПА,
  - ключ К;
- зашифровывают блок данных ДЗ на модифицированном ключе КЗ, получая модифицированное значение зашифрованных данных ШДЗ;
- заменяют в учетной записи пользователя УЗ значение зашифрованных данных ШДЗ на модифицированное значение;

при необходимости со стороны администратора объекта проведения проверки учетной записи пользователя выполняют следующие действия:

- выполняют действия для доступа к защищаемому объекту согласно этапу А, получая ключи КА и КО;
- получают из списка доступа проверяемую учетную запись пользователя УЗ;
- из учетной записи УЗ получают значения зашифрованных данных ШДЗ, ШДА;
- расшифровывают данные ШДА на ключе КА, получая ключ КЗ, параметр ПА и текстовое описание Т учетной записи УЗ;
- расшифровывают данные ШДЗ на ключе КЗ, получая параметр ПА и ключ К;
- по текстовому описанию Т устанавливают соответствие сведений учетной записи УЗ пользователю, имеющему допуск к защищаемому объекту;
- устанавливают соответствие значений параметра ПА, полученных из данных ШДА и ШДЗ;
- если параметр ПА указывает на наличие у пользователя полномочий администратора, устанавливают соответствие ключа К ключу КА;
- если параметр ПА указывает на отсутствие у пользователя полномочий администратора, устанавливают соответствие ключа К ключу КО;

при необходимости со стороны администратора объекта замены ключа шифрования данных выполняют следующие действия:

- выполняют действия для доступа к защищаемому объекту согласно этапу А, получая ключи КА, КО и идентификатор ИД;
- расшифровывают на ключе КО данные ШДО, получая данные защищаемого объекта ДО;
- генерируют случайный модифицированный симметричный ключ администрирования объекта КА;
- вычисляют производный ключ для модифицированного ключа КА, используя идентификатор ИД в качестве модификатора, получая модифицированный ключ КО;
- зашифровывают данные ДО на модифицированном ключе КО;

- формируют модифицированный список доступа ДД к объекту, выполняя для каждой учетной записи пользователя УЗ из списка доступа ДД следующие действия:
  - считывают значение идентификатора ИЗ;
  - выполняют проверку учетной записи пользователя УЗ, получая при этом значения идентификатора ИЗ, ключа ОКП, параметра ПА и текстовое описание Т;
  - при неуспешной проверке исключают УЗ из модифицированного списка доступа ДД и переходят к следующей учетной записи, иначе выполняют следующие действия:
    - генерируют случайную модифицированную асимметричную пару ключей в составе открытого ключа ОКЗ и секретного ключа СКЗ;
    - генерируют случайный модифицированный симметричный ключ КЗ;
    - вычисляют модифицированное значение общего ключа КЗП из модифицированного ключа СКЗ и ключа ОКП;
    - зашифровывают модифицированный ключ КЗ на модифицированном ключе КЗП, получая модифицированное значение зашифрованного ключа ШКЗ;
    - формируют модифицированный блок данных ДЗ из следующих данных:
      - ключ ОКП,
      - параметр ПА,
      - модифицированный ключ КА, если параметр ПА указывает на наличие у пользователя полномочий администратора, иначе - модифицированный ключ КО;
    - зашифровывают модифицированный блок данных ДЗ на модифицированном ключе КЗ, получая модифицированное значение зашифрованных данных ШДЗ;
    - формируют модифицированный блок проверочных данных ДА из следующих данных:
      - модифицированный ключ КЗ,
      - параметр ПА,
      - текстовое описание Т;
    - зашифровывают модифицированный блок ДА на модифицированном ключе КА, получая модифицированное значение зашифрованных данных ШДА;
    - формируют учетную запись УЗ в модифицированном списке доступа ДД из следующих данных:
      - идентификатор ИЗ,
      - модифицированный ключ ОКЗ,
      - модифицированный зашифрованный ключ ШКЗ,
      - модифицированные зашифрованные данные ШДЗ.

Заявляемый способ применим в условиях, когда объект с защищаемой информацией и списки доступа к нему располагаются в общедоступном месте. Вместе с тем, допускается использование дополнительных мер защиты для доступа к объекту и его спискам доступа, что находится за рамками заявляемого способа.

В заявляемом способе управление доступом к защищаемой информации осуществляется путем предоставления легитимному пользователю возможности вычислить секретный параметр (ключ) КО, на котором зашифрованы данные объекта. Известны многочисленные классические (симметричные) алгоритмы шифрования и режимы их работы, обеспечивающие соответствующие характеристики защиты информации (Шнайер Б. Прикладная криптография, М: Триумф, 2002 г.). В заявляемом способе не имеет значения, какой именно алгоритм шифрования используется для защиты информации. От применяемого алгоритма шифрования и режима его использования требуется только то, что без знания секретного ключа в зашифрованном тексте нельзя заменить отдельные фрагменты, целенаправленно навязав нужные данные

при расшифровании.

Для разделения ролей пользователей и администраторов в заявляемом способе используется диверсификация ключей: администратору предоставляется главный ключ - ключ администрирования КА, а пользователь оперирует с производным ключом КО, формируемым из ключа администрирования и несекретного модификатора - уникального идентификатора объекта ИД - с помощью однонаправленной функции NewKey (КА, ИД) = КО. Применение однонаправленной функции NewKey () обеспечивает невозможность пользователю по известному ключу КО вычислить ключ администрирования КА и получить привилегии администратора, предоставляемые этим ключом. Подобная диверсификация ключей применима для выделения роли суперпользователя из администраторов или дифференцирования ролей пользователей. Известно много функций диверсификации ключей, например, (RFC 8018, NIST Special Publication 800-132, Р 50.1.113-2016, информация по адресу: https://tools.ietf.org/html/rfc8018). Для заявляемого способа не имеет значения, какая из функций диверсификации ключей используется.

Одной из отличительных особенностей заявляемого способа является разделение учетной записи пользователя на две связанные между собой части с разными правами доступа. К первой части учетной записи получают доступ администратор и легитимный пользователь, а ко второй - исключительно администратор. Исключительный доступ администратора ко второй части учетной записи позволяют ему размещать в ней данные для контроля легитимности изменений, дозволяемых вносить пользователем в первую часть учетной записи.

Другой отличительной особенностью заявляемого способа является шифрование каждой из частей учетной записи пользователя на отдельных ключах. Раздельное шифрование частей учетной записи не только обеспечивает разделение полномочий на доступ к ним между пользователем и администратором, но и позволяет скрыть от остальных пользователей принадлежность этой учетной записи конкретному лицу и используемые им параметры авторизации в этой записи.

Для совместного доступа администратора и пользователя к общей части учетной записи в заявляемом способе применяются эфемерные ключи (NIST Special Publication 800-57 Revivsion 3, Р 50.1.113-2016, информация по адресу: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf) для системы открытого распределения ключей. Система открытого распределения ключей является разновидностью систем с открытым ключом, в которой пара пользователей, обладающие открытыми ключами друг друга ОКП1 и ОКП2, эффективно вычисляют с помощью общеизвестной функции ComKey () общий секретный ключ К12 без дополнительного взаимодействия между собой, используя свои секретные ключи СКП1 и СКП2, как:

К12 = ComKey (ОКП2, СКП1) и

К12 = ComKey (ОКП1, СКП2).

От системы открытого распределения ключей требуется, чтобы нахождение общего ключа К12 только по открытым ключам ОКП1 и ОКП2 без использования ключей СКП1 или СКП2 было неприемлемо сложной вычислительной задачей.

Известно несколько систем открытого распределения ключей, из которых наибольшее распространение получила система Диффи-Хеллмана (патент США №4200770, приоритет от 06.09.1977 г.). Для заявляемого способа не имеет значения, какая из систем открытого распределения ключей используется.

В заявляемом способе списки доступа к защищаемому информационному объекту формируются администратором объекта следующим образом.

По правилам операционной системы (ОС), используемой в компьютере, защищаемому объекту присваивается уникальный идентификатор ИД (для ОС Windows, например, размер уникального идентификатора составляет 16 байт).

Формируется служебная информация защищаемого объекта ДС, содержащая открытую информацию вида: тип объекта, форматы данных объекта, номер версии программного обеспечения (ПО), спецификации используемых криптографических преобразований СФ и уникальный идентификатор ИД. Состав служебной информации не имеет принципиального значения для заявляемого способа.

Генерируется случайный симметричный ключ администрирования КА = rand(), из которого с помощью однонаправленной функции диверсификации ключей NewKey(*,*) по уникальному идентификатору объекта ИД вычисляется производный ключ - ключ защиты объекта КО = NewKey (КА, ИД).

Информация защищаемого объекта ДО зашифровывается на ключе защиты объекта КО и замещается зашифрованными данными ШДО = Encrypt (ДО, КО).

Вместе с зашифрованными данными хранится служебная информация и список доступа, состоящий из учетных записей пользователей. Учетные записи пользователей и администраторов создаются администратором на основании персональных открытых ключей пользователей ОКП.

Для создания учетной записи пользователя администратор генерирует случайный симметричный ключ учетной записи КЗ = rand () и генерирует асимметричную пару из открытого и секретного ключей записи (ОКЗ, СКЗ) = GenPub (rand()), где GenPub (*) - функция генерации пары ключей для системы открытого распределения ключей, а rand() - датчик случайных чисел.

По открытому ключу пользователя ОКП и сгенерированному эфемерному ключу СКЗ, администратором вычисляется общий ключ КЗП = ComKey (ОКП, СКЗ), где = ComKey (*,*) - функция формирования общего парного ключа.

В учетную запись пользователя помещается открытый ключ ОКП и результат ШКЗ зашифровывания на общем ключе КЗП ключа учетной записи КЗ, т.е. ШКЗ = Encrypt (КЗ, КЗП).

К учетной записи добавляются зашифрованные на ключе учетной записи КЗ данные записи пользователя ДЗ, состоящие из значений: открытого ключа пользователя ОКП, характеризующего роль пользователя параметра ПА (администратор или пользователь), и ключа К, в качестве которого для роли администратора выступает КА, а для роли пользователя - КО, т.е. ШДЗ = Encrypt (ОКП || ПА || К, КЗ).

Для проверки подлинности учетной записи в нее включается блок проверочных данных администрирования ДА - ключ учетной записи КЗ, роль пользователя ПА и текстовая информация о пользователе Т, зашифрованный на ключе администрирования КА : ШДА = Encrypt (КЗ || ПА || Т, КА).

Для предоставления пользователю возможности эффективного поиска своей учетной записи, каждая из них при создании снабжается временным идентификатором ВИ, получаемым случайно: ВИ = rand (). При первом обращении пользователя к защищаемому объекту он заменяет временный идентификатор ВИ на постоянный идентификатор учетной записи ИЗ, вычисленный им с помощью однонаправленной функции Hash от уникального идентификатора объекта ИД и ключа, получаемого как общий ключ для своих секретного и отрытого ключей КПП = ComKey (ОКП, СКП):

ИЗ = Hash (ИД || КПП).

Таким образом, в заявляемом способе управления вместе с защищаемыми данными объекта хранится уникальный идентификатор объекта ИД и спецификации форматов/

алгоритмов СФ, а данные объекта зашифрованы на симметричном ключе КО, являющемся производным симметричным ключом КО = NewKey (КА, ИД) от случайно сгенерированного ключа администрирования КА = rand ().

В списке доступа каждая учетная запись пользователя, включая администратора защищаемого объекта, имеет уникальный идентификатор ИЗ, вычисленный с помощью однонаправленной функции, как ИЗ = Hash (ИД || КПП), где КПП - секретный ключ, полученный как общий ключ для открытого и секретного ключей пользователя, КПП = ComKey (ОКП, СКП), или случайный временный идентификатор ВИ, назначаемый администратором для первого сеанса работы пользователя.

Каждая учетная запись содержит значения:

- ОКЗ - открытый ключ из случайно сгенерированной пары открытого и секретного ключей (ОКЗ, СКЗ) = GenPub (rand ());
- ШКЗ = Encrypt (КЗП, КЗ) - случайно сгенерированный симметричный ключ записи КЗ = rand (), зашифрованный на общем ключе КЗП, вычисленного в системе открытого распределения ключей КЗП = ComKey (ОКП, СКЗ) по открытому ключу пользователя ОКП и ключу СКЗ;
- ШДЗ = Encrypt (ОКП || ПА || К, КЗ) - зашифрованная на ключе записи КЗ информация пользователя, состоящая из открытого ключа пользователя ОКП, параметра ПА, характеризующего роль пользователя (администратор или пользователь) и симметричного ключа К, который для роли администратора является КА, а для роли пользователя - КО.
- ШДА=Encrypt (КЗ || ПА || Т, КА) - зашифрованные на ключе администрирования КА проверочные данные, состоящие из ключа записи КЗ, параметра ПА, характеризующего роль пользователя (администратор или пользователь) и текстового описания о пользователе Т.

Для доступа к защищаемому объекту пользователь извлекает из служебной информации уникальный идентификатор объекта ИД и вычисляет сначала ключ КПП = ComKey (ОКП, СКП), а затем идентификатор своей записи как ИЗ = Hash (ИД || КПП). При первом обращении к объекту использует вместо ИЗ случайный временный идентификатор ВИ, назначаемый ему администратором. По идентификатору пользователь находит свою учетную запись, а при первом обращении к объекту самостоятельно заменяет идентификатор ВИ на постоянное значение ИЗ.

Далее пользователь извлекает из своей учетной записи открытый ключ записи ОКЗ и, используя свой секретный ключ СКП, вычисляет общий ключ КЗП = ComKey (ОКЗ, СКП), на котором расшифровывает поле ШКЗ и находит ключ записи КЗ = Decrypt (ШКЗ, КЗП). На ключе записи КЗ пользователь расшифровывает поле ШДЗ и находит значения ОКП || ПА || К = Decrypt (ШДЗ, КЗ). Если параметр ПА указывает на роль «пользователь», то К = КО и пользователь получает доступ к данным объекта, расшифровывая их на ключе К. Если роль «администратор», то К = КА, и пользователь для расшифровывания данных объекта вычисляет производный ключ КО = NewKey (КА, ИД).

Для перехода на новую пару открытого и секретного ключа (ОКМ, СКМ) пользователь осуществляет описанные выше вычисления с прежней парой ключей (ОКП, СКП) и вычисляет новые значения:

КПП = ComKey (ОКМ, СКМ),

ИЗ = Hash (ИД || КПП),

ШДЗ = Encrypt (ОКМ || ПА || К, КЗ),

ШКЗ = Encrypt (КЗ, КЗП),

где КЗП = ComKey (ОКЗ, СКМ),

и заменяет в учетной записи прежние значения на соответствующие новые.

Для проверки подлинности учетной записи пользователя администратор выполняет описанные выше вычисления со своей учетной записью и находит значения КА и КО. Затем на ключе КА расшифровывает поле ШДА в учетной записи пользователя и получает значения КЗ || ПА || Т = Decrypt (ДА, КА). После чего в той же учетной записи расшифровывает на полученном ключе КЗ поле ШДЗ, находит значения ОКП || ПА || К = Decrypt (ШДЗ, КЗ) и проверяет совпадение определяющего роль пользователя параметра ПА с ранее расшифрованной и совпадение К с КА или с КО в соответствии с ролью пользователя.

Для смены ключа шифрования объекта администратор генерирует новый случайный ключ администрирования КА = rand() и вычисляет новый ключ объекта КО = NewKey (КА, ИД), после чего по своей учетной записи, как описано выше, находит прежние ключи КА и КО и перешифровывает данные объекта с прежнего ключа на новый. После чего проверяет каждую учетную запись пользователя описанным выше способом. В прошедших проверку записях сохраняется идентификатор записи пользователя ИЗ, а остальные поля пересчитываются для новых значений по предлагаемым формулам.

Делегирование полномочий администратора пользователю состоит в том, что при формировании полей ШДЗ и ШДА параметр ПА указывает на роль «администратор», а параметр К = КА.

Формирование идентификатора учетной записи пользователя на основе уникального идентификатора объекта ИД обеспечивает неповторимость этого идентификатора для разных объектов даже при использовании пользователем одного и того же ключа для доступа к объекту.

Поскольку данные об открытом ключе пользователя зашифрованы на индивидуальном для каждой записи ключе КЗ, а этот ключ может вычислить только администратор или сам пользователь, то выявить повторение открытого ключа в 2-х списках доступа может только администратор обоих списков или сам пользователь, что обеспечивает сохранение в тайне состава лиц, имеющих доступ к защищаемому объекту.

Осуществление изобретения

Реализация предложенного способа может быть осуществлена в компьютере, работающем под управлением любой ОС, например, Windows 7, 10 и др.

В компьютере должен быть определен администратор и пользователи, внесенные в список (по крайней мере один пользователь).

Администратор должен иметь возможность, при необходимости, получить у пользователей, которые предварительно сформировали асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, их открытые ключи ОКП.

В компьютере должен также присутствовать защищаемый объект по крайней мере один, доступ к которому целесообразно защищать, например, это может быть текстовый файл с конфиденциальной информацией.

Для подготовки к использованию предлагаемого способа необходимо сформировать программное средство, выполненное с возможностью

- генерировать уникальные идентификаторы,
- генерировать случайные числа,
- генерировать случайные симметричные ключи,
- генерировать случайные асимметричные пары ключей в составе открытого ключа и секретного ключа,

- вычислять значение функции хэширования,
- вычислять производный симметричный ключ из исходного симметричного ключа и значения модификатора,
- вычислять общий симметричный ключ из секретного ключа и открытого ключа,
- зашифровывать и расшифровывать данные на симметричном ключе,
- зашифровывать и расшифровывать симметричный ключ на симметричном ключе.

Это программное средство представляет собой программу или комплекс программ, которую, зная ее назначение и выполняемые функции, может сформировать специалист в области программирования (программист). Подготовленное программное средство после сформирования устанавливается (инсталлируется) в компьютер.

Затем на компьютере начинается работа в обычном режиме. В ходе работы со стороны администратора защищаемого объекта с данными объекта ДО выполняют следующие действия:

- генерируют уникальный идентификатор ИД защищаемого объекта;
- генерируют случайный симметричный ключ КА администрирования объекта;
- получают симметричный ключ шифрования данных объекта КО путем вычисления производного ключа от ключа КА с использованием идентификатора ИД в качестве модификатора;
- зашифровывают данные защищаемого объекта ДО на ключе КО, получая зашифрованные данные ШДО;
- формируют блок данных служебной информации ДС, содержащий идентификатор ИД, сведения о защищаемом объекте и спецификацию использующихся криптографических функций СФ;
- формируют список доступа ДД к объекту, состоящий из учетных записей пользователей, которым предоставляется доступ к защищаемому объекту, причем по крайней мере одна из учетных записей принадлежит администратору объекта, выполняя для каждой учетной записи УЗ следующие действия:
  - получают у выбранного пользователя, имеющего асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, его открытый ключ ОКП;
  - генерируют случайное число, принимают его в качестве временного идентификатора ВИ;
  - формируют идентификатор ИЗ учетной записи УЗ, принимая в качестве его значения временный идентификатор ВИ;
  - генерируют случайную асимметричную пару ключей в составе открытого ключа ОКЗ и секретного ключа СКЗ;
  - генерируют случайный симметричный ключ КЗ учетной записи УЗ;
  - вычисляют общий симметричный ключ КЗП из секретного ключа СКЗ и открытого ключа ОКП;
  - зашифровывают ключ КЗ на ключе КЗП, получая зашифрованный ключ ШКЗ;
  - принимают решение о наделении пользователя полномочиями администратора;
  - формируют значение параметра ПА, характеризующего наличие у пользователя полномочий администратора;
  - формируют блок данных ДЗ из следующих данных:
    - ключ ОКП,
    - параметр ПА,
    - ключ КА, если параметр ПА указывает на наличие у пользователя полномочий администратора, иначе - ключ КО;
  - зашифровывают блок данных ДЗ на ключе КЗ, получая зашифрованные данные

ШДЗ;

- формируют текстовое описание Т учетной записи УЗ выбранного пользователя;
- формируют блок проверочных данных администрирования ДА из следующих данных:
  - ключ КЗ,
  - параметр ПА,
  - текстовое описание Т;
- зашифровывают блок данных ДА на ключе КА, получая зашифрованные данные ШДА;
- формируют учетную запись выбранного пользователя УЗ в виде следующего блока данных:
  - идентификатор ИЗ,
  - ключ ОКЗ,
  - зашифрованный ключ ШКЗ,
  - зашифрованные данные ШДЗ,
  - зашифрованные данные ШДА;
- сохраняют совместно следующие данные:
- зашифрованные данные ШДО,
- служебную информацию ДС,
- список доступа к объекту ДД.

Таким образом, получают данные объекта ДО в защищенном, зашифрованном виде.

Используемый при обеспечении доступа к защищаемому объекту параметр ПА может представлять собой, например, целое число 0 или 1 (где 0 обозначает отсутствие у пользователя полномочий администратора, а 1 - наличие у пользователя таких полномочий) или текст вида "Yes" или "No" с соответствующим смыслом.

При этом обеспечивается также дифференциации ролей пользователей путем выделение ролей администраторов с возможностью делегирования прав администратора другим пользователям.

В качестве сведений о защищаемом объекте в составе блока данных служебной информации ДС может быть использовано текстовое описание объекта, например, текст вида "Перечень программных модулей".

В качестве спецификации использующихся криптографических функций СФ могут быть использованы:

- применяемый алгоритм симметричного шифрования, длина блока и длина ключей, например блочный шифр «Кузнечик» по ГОСТ Р 34.12-2015 с длиной блока 128 бит и длиной ключа 256 бит, или блочный шифр AES по FIPS PUB 197 Advanced Encryption Standard с длиной блока 128 бит и длиной ключа 256 бит;
- применяемый алгоритм хэширования и размер хэширования, например? функция хэширования ГОСТ Р 34.11-2012 с размером хэша 256 бит или SHA-256 по FIPS PUB 180-4 Secure Hash Standard с размером хэша 256 бит;
- применяемый алгоритм получения производного ключа, например, функция KDF_GOSTR3411_2012_256 по Р 50.1.113-2016, или HKDF по RFC 5869, и их параметры и др.

При необходимости доступа к защищаемому объекту со стороны пользователя, имеющего асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, выполняют следующие действия:

- (А) извлекают из служебной информации ДС идентификатор объекта ИД и спецификацию использующихся криптографических функций СФ;

- вычисляют общий симметричный ключ КПП из секретного ключа СКП и открытого ключа ОКП;
- вычисляют значение функции хэширования от блока данных, составленного из идентификатора ИД и ключа КПП, получая постоянное значение идентификатора ИЗ;
- если доступ выполняется в первый раз с момента формирования администратором объекта списка доступа, то переходят к этапу (Б), иначе переходят к этапу (В);
- (Б) получают у администратора объекта временный идентификатор ВИ, назначенный учетной записи данного пользователя при первичном формировании списка доступа;
- находят в списке доступа ДД учетную запись, у которой значение идентификатора ИЗ совпадает с ВИ;
- заменяют в учетной записи пользователя значение идентификатора ИЗ на вычисленное постоянное значение;
- (В) находят в списке доступа ДД учетную запись, у которой значение ИЗ совпадает с вычисленным;
- получают из найденной учетной записи ключи ОКЗ, ШКЗ и зашифрованные данные ШДЗ, ШДА;
- вычисляют общий симметричный ключ КЗП из ключей СКП и ОКЗ;
- расшифровывают ключом КЗП зашифрованный ключ ШКЗ, получая секретный ключ КЗ;
- расшифровывают ключом КЗ зашифрованные данные ШДЗ, получая значение параметра ПА и ключ К;
- если параметр ПА указывает на наличие у пользователя полномочий администратора, принимают ключ К в качестве ключа администрирования КА и вычисляют для него производный ключ, используя идентификатор ИД в качестве модификатора, получая ключ шифрования данных КО;
- если параметр ПА указывает на отсутствие у пользователя полномочий администратора, принимают ключ К в качестве ключа шифрования данных КО;
- расшифровывают зашифрованные данные ШДО с помощью ключа КО, получая данные защищаемого объекта ДО;

Таким образом, обеспечивается доступ к данным, как для обычных пользователей, так и для пользователей с правами администраторов, и, кроме того, децентрализованный контроль над правами доступа путем предоставление доступа к информации по результатам локальной авторизации пользователей без использования доверенных централизованных сервисов авторизации.

При необходимости со стороны пользователя, имеющего асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, перейти на использование другой асимметричной пары ключей в составе открытого ключа ОКМ и секретного ключа СКМ и иметь доступ к защищаемому объекту, выполняют следующие действия:

- выполняют действия для доступа к защищаемому объекту согласно этапу А, получая идентификатор ИД, ключи ОКЗ, КЗ, К и значение параметра ПА;
- вычисляют общий симметричный ключ КММ из секретного ключа СКМ и открытого ключа ОКМ;
- вычисляют значение функции хэширования от блока данных, составленного из идентификатора ИД и ключа КММ, получая модифицированное постоянное значение идентификатора ИЗ;
- заменяют в учетной записи пользователя УЗ значение идентификатора ИЗ на

модифицированное значение;

- вычисляют модифицированное значение ключа КЗП как общий симметричный ключ для ключей СКМ и ОКЗ;
- зашифровывают ключ КЗ на модифицированном ключе КЗП, получая модифицированное значение зашифрованного ключ ШКЗ;
- заменяют в учетной записи пользователя УЗ значение зашифрованного ключа ШКЗ на модифицированное значение;
- формируют модифицированный блок данных ДЗ из следующих данных:
  - ключ ОКМ,
  - параметр ПА,
  - ключ К;
- зашифровывают блок данных ДЗ на модифицированном ключе КЗ, получая модифицированное значение зашифрованных данных ШДЗ;
- заменяют в учетной записи пользователя УЗ значение зашифрованных данных ШДЗ на модифицированное значение.

В результате, обеспечивается эффективный поиск для пользователей своей учетной записи в списке доступа и независимая смена параметров защиты объекта, при которой замена администратором параметров защиты информации не требует взаимодействия с пользователями и другими администраторами.

При необходимости со стороны администратора объекта проведения проверки учетной записи пользователя выполняют следующие действия:

- выполняют действия для доступа к защищаемому объекту согласно этапу А, получая ключи КА и КО;
- получают из списка доступа проверяемую учетную запись пользователя УЗ;
- из учетной записи УЗ получают значения зашифрованных данных ШДЗ, ШДА;
- расшифровывают данные ШДА на ключе КА, получая ключ КЗ, параметр ПА и текстовое описание Т учетной записи УЗ;
- расшифровывают данные ШДЗ на ключе КЗ, получая параметр ПА и ключ К;
- по текстовому описанию Т устанавливают соответствие сведений учетной записи УЗ пользователю, имеющему допуск к защищаемому объекту;
- устанавливают соответствие значений параметра ПА, полученных из данных ШДА и ШДЗ;
- если параметр ПА указывает на наличие у пользователя полномочий администратора, устанавливают соответствие ключа К ключу КА;
- если параметр ПА указывает на отсутствие у пользователя полномочий администратора, устанавливают соответствие ключа К ключу КО.

Таким образом, обеспечивается выявление несанкционированных изменений в списке доступа, возможность коррекции и сокрытия состава лиц, имеющих доступ к защищаемой информации.

При необходимости со стороны администратора объекта замены ключа шифрования данных выполняют следующие действия:

- выполняют действия для доступа к защищаемому объекту согласно этапу А, получая ключи КА, КО и идентификатор ИД;
- расшифровывают на ключе КО данные ШДО, получая данные защищаемого объекта ДО;
- генерируют случайный модифицированный симметричный ключ администрирования объекта КА;
- вычисляют производный ключ для модифицированного ключа КА, используя

идентификатор ИД в качестве модификатора, получая модифицированный ключ КО;

- зашифровывают данные ДО на модифицированном ключе КО;
- формируют модифицированный список доступа ДД к объекту, выполняя для каждой учетной записи пользователя УЗ из списка доступа ДД следующие действия:
  - считывают значение идентификатора ИЗ;
  - выполняют проверку учетной записи пользователя УЗ, получая при этом значения идентификатора ИЗ, ключа ОКП, параметра ПА и текстовое описание Т;
  - при неуспешной проверке исключают УЗ из модифицированного списка доступа ДД и переходят к следующей учетной записи, иначе выполняют следующие действия:
    - генерируют случайную модифицированную асимметричную пару ключей в составе открытого ключа ОКЗ и секретного ключа СКЗ;
    - генерируют случайный модифицированный симметричный ключ КЗ;
    - вычисляют модифицированное значение общего ключа КЗП из модифицированного ключа СКЗ и ключа ОКП;
    - зашифровывают модифицированный ключ КЗ на модифицированном ключе КЗП, получая модифицированное значение зашифрованного ключа ШКЗ;
    - формируют модифицированный блок данных ДЗ из следующих данных:
      - ключ ОКП,
      - параметр ПА,
      - модифицированный ключ КА, если параметр ПА указывает на наличие у пользователя полномочий администратора, иначе - модифицированный ключ КО;
    - зашифровывают модифицированный блок данных ДЗ на модифицированном ключе КЗ, получая модифицированное значение зашифрованных данных ШДЗ;
    - формируют модифицированный блок проверочных данных ДА из следующих данных:
      - модифицированный ключ КЗ,
      - параметр ПА,
      - текстовое описание Т;
    - зашифровывают модифицированный блок ДА на модифицированном ключе КА, получая модифицированное значение зашифрованных данных ШДА;
    - формируют учетную запись УЗ в модифицированном списке доступа ДД из следующих данных:
      - идентификатор ИЗ,
      - модифицированный ключ ОКЗ,
      - модифицированный зашифрованный ключ ШКЗ,
      - модифицированные зашифрованные данные ШДЗ.

Таким образом, обеспечивается независимая смена параметров защиты объекта, при которой замена администратором параметров защиты информации не требует взаимодействия с пользователями и другими администраторами.

(57) Формула изобретения

Способ управления доступом к данным в компьютере, причем компьютер имеет установленное программное средство, выполненное с возможностью

генерировать уникальные идентификаторы,

генерировать случайные числа,

генерировать случайные симметричные ключи,

генерировать случайные асимметричные пары ключей в составе открытого ключа и секретного ключа,

вычислять значение функции хэширования,

вычислять производный симметричный ключ из исходного симметричного ключа и значения модификатора,

вычислять общий симметричный ключ из секретного ключа и открытого ключа,

зашифровывать и расшифровывать данные на симметричном ключе,

зашифровывать и расшифровывать симметричный ключ на симметричном ключе,

способ заключается в том, что со стороны администратора защищаемого объекта с данными объекта ДО выполняют следующие действия:

генерируют уникальный идентификатор ИД защищаемого объекта;

генерируют случайный симметричный ключ КА администрирования объекта;

получают симметричный ключ шифрования данных объекта КО путем вычисления производного ключа от ключа КА с использованием идентификатора ИД в качестве модификатора;

зашифровывают данные защищаемого объекта ДО на ключе КО, получая зашифрованные данные ШДО;

формируют блок данных служебной информации ДС, содержащий идентификатор ИД, сведения о защищаемом объекте и спецификацию использующихся криптографических функций СФ;

формируют список доступа ДД к объекту, состоящий из учетных записей пользователей, которым предоставляется доступ к защищаемому объекту, причем по крайней мере одна из учетных записей принадлежит администратору объекта, выполняя для каждой учетной записи УЗ следующие действия:

получают у выбранного пользователя, имеющего асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, его открытый ключ ОКП;

генерируют случайное число, принимают его в качестве временного идентификатора ВИ;

формируют идентификатор ИЗ учетной записи УЗ, принимая в качестве его значения временный идентификатор ВИ;

генерируют случайную асимметричную пару ключей в составе открытого ключа ОКЗ и секретного ключа СКЗ;

генерируют случайный симметричный ключ КЗ учетной записи УЗ;

вычисляют общий симметричный ключ КЗП из секретного ключа СКЗ и открытого ключа ОКП;

зашифровывают ключ КЗ на ключе КЗП, получая зашифрованный ключ ШКЗ;

принимают решение о наделении пользователя полномочиями администратора;

формируют значение параметра ПА, характеризующего наличие у пользователя полномочий администратора;

формируют блок данных ДЗ из следующих данных:

ключ ОКП,

параметр ПА,

ключ КА, если параметр ПА указывает на наличие у пользователя полномочий администратора, иначе - ключ КО;

зашифровывают блок данных ДЗ на ключе КЗ, получая зашифрованные данные ШДЗ;

формируют текстовое описание Т учетной записи УЗ выбранного пользователя;

формируют блок проверочных данных администрирования ДА из следующих данных:

ключ КЗ,

параметр ПА,

текстовое описание Т;

зашифровывают блок данных ДА на ключе КА, получая зашифрованные данные ШДА;

формируют учетную запись выбранного пользователя УЗ в виде следующего блока данных:

идентификатор ИЗ,

ключ ОКЗ,

зашифрованный ключ ШКЗ,

зашифрованные данные ШДЗ,

зашифрованные данные ШДА;

сохраняют совместно следующие данные:

- зашифрованные данные ШДО,

- служебную информацию ДС,

- список доступа к объекту ДД;

при необходимости доступа к защищаемому объекту со стороны пользователя, имеющего асимметричную пару ключей в составе открытого ключа ОКП и секретного ключа СКП, выполняют следующие действия:

(А) извлекают из служебной информации ДС идентификатор объекта ИД и спецификацию использующихся криптографических функций СФ;

вычисляют общий симметричный ключ КПП из секретного ключа СКП и открытого ключа ОКП;

вычисляют значение функции хэширования от блока данных, составленного из идентификатора ИД и ключа КПП, получая постоянное значение идентификатора ИЗ;

если доступ выполняется в первый раз с момента формирования администратором объекта списка доступа, то переходят к этапу (Б), иначе переходят к этапу (В);

(Б) получают у администратора объекта временный идентификатор ВИ, назначенный учетной записи данного пользователя при первичном формировании списка доступа;

находят в списке доступа ДД учетную запись, у которой значение идентификатора ИЗ совпадает с ВИ;

заменяют в учетной записи пользователя значение идентификатора ИЗ на вычисленное постоянное значение;

(В) находят в списке доступа ДД учетную запись, у которой значение ИЗ совпадает с вычисленным;

получают из найденной учетной записи ключи ОКЗ, ШКЗ и зашифрованные данные ШДЗ, ШДА;

вычисляют общий симметричный ключ КЗП из ключей СКП и ОКЗ; расшифровывают ключом КЗП зашифрованный ключ ШКЗ, получая секретный ключ КЗ;

расшифровывают ключом КЗ зашифрованные данные ШДЗ, получая значение параметра ПА и ключ К;

если параметр ПА указывает на наличие у пользователя полномочий администратора, принимают ключ К в качестве ключа администрирования КА и вычисляют для него производный ключ, используя идентификатор ИД в качестве модификатора, получая ключ шифрования данных КО;

если параметр ПА указывает на отсутствие у пользователя полномочий администратора, принимают ключ К в качестве ключа шифрования данных КО;

расшифровывают зашифрованные данные ШДО с помощью ключа КО,

получая данные защищаемого объекта ДО;

при необходимости со стороны пользователя, имеющего асимметричную пару ключей

в составе открытого ключа ОКП и секретного ключа СКП, перейти на использование другой асимметричной пары ключей в составе открытого ключа ОКМ и секретного ключа СКМ и иметь доступ к защищаемому объекту, выполняют следующие действия:

выполняют действия для доступа к защищаемому объекту согласно этапу А, получая идентификатор ИД, ключи ОКЗ, КЗ, К и значение параметра ПА;

вычисляют общий симметричный ключ КММ из секретного ключа СКМ и открытого ключа ОКМ;

вычисляют значение функции хэширования от блока данных, составленного из идентификатора ИД и ключа КММ, получая модифицированное постоянное значение идентификатора ИЗ;

заменяют в учетной записи пользователя УЗ значение идентификатора ИЗ на модифицированное значение;

вычисляют модифицированное значение ключа КЗП как общий симметричный ключ для ключей СКМ и ОКЗ;

зашифровывают ключ КЗ на модифицированном ключе КЗП, получая модифицированное значение зашифрованного ключ ШКЗ;

заменяют в учетной записи пользователя УЗ значение зашифрованного ключа ШКЗ на модифицированное значение;

формируют модифицированный блок данных ДЗ из следующих данных:

ключ ОКМ,

параметр ПА,

ключ К;

зашифровывают блок данных ДЗ на модифицированном ключе КЗ, получая модифицированное значение зашифрованных данных ШДЗ;

заменяют в учетной записи пользователя УЗ значение зашифрованных данных ШДЗ на модифицированное значение;

при необходимости со стороны администратора объекта проведения проверки учетной записи пользователя выполняют следующие действия:

выполняют действия для доступа к защищаемому объекту согласно этапу А, получая ключи КА и КО;

получают из списка доступа проверяемую учетную запись пользователя УЗ;

из учетной записи УЗ получают значения зашифрованных данных ШДЗ, ШДА;

расшифровывают данные ШДА на ключе КА, получая ключ КЗ, параметр ПА и текстовое описание Т учетной записи УЗ;

расшифровывают данные ШДЗ на ключе КЗ, получая параметр ПА и ключ К;

по текстовому описанию Т устанавливают соответствие сведений учетной записи УЗ пользователю, имеющему допуск к защищаемому объекту; устанавливают соответствие значений параметра ПА, полученных из данных ШДА и ШДЗ;

если параметр ПА указывает на наличие у пользователя полномочий администратора, устанавливают соответствие ключа К ключу КА;

если параметр ПА указывает на отсутствие у пользователя полномочий администратора, устанавливают соответствие ключа К ключу КО;

при необходимости со стороны администратора объекта замены ключа шифрования данных выполняют следующие действия:

выполняют действия для доступа к защищаемому объекту согласно этапу А, получая ключи КА, КО и идентификатор ИД;

расшифровывают на ключе КО данные ШДО, получая данные защищаемого объекта ДО;

генерируют случайный модифицированный симметричный ключ администрирования объекта КА;

вычисляют производный ключ для модифицированного ключа КА, используя идентификатор ИД в качестве модификатора, получая модифицированный ключ КО;

зашифровывают данные ДО на модифицированном ключе КО;

формируют модифицированный список доступа ДД к объекту, выполняя для каждой учетной записи пользователя УЗ из списка доступа ДД следующие действия:

считывают значение идентификатора ИЗ;

выполняют проверку учетной записи пользователя УЗ, получая при этом значения идентификатора ИЗ, ключа ОКП, параметра ПА и текстовое описание Т;

при неуспешной проверке исключают УЗ из модифицированного списка доступа ДД и переходят к следующей учетной записи, иначе выполняют следующие действия:

генерируют случайную модифицированную асимметричную пару ключей в составе открытого ключа ОКЗ и секретного ключа СКЗ;

генерируют случайный модифицированный симметричный ключ КЗ;

вычисляют модифицированное значение общего ключа КЗП из модифицированного ключа СКЗ и ключа ОКП;

зашифровывают модифицированный ключ КЗ на модифицированном ключе КЗП, получая модифицированное значение зашифрованного ключа ШКЗ;

формируют модифицированный блок данных ДЗ из следующих данных:

ключ ОКП,

параметр ПА,

модифицированный ключ КА, если параметр ПА указывает на наличие у пользователя полномочий администратора, иначе - модифицированный ключ КО;

зашифровывают модифицированный блок данных ДЗ на модифицированном ключе КЗ, получая модифицированное значение зашифрованных данных ШДЗ;

формируют модифицированный блок проверочных данных ДА из следующих данных:

модифицированный ключ КЗ,

параметр ПА,

текстовое описание Т;

зашифровывают модифицированный блок ДА на модифицированном ключе КА, получая модифицированное значение зашифрованных данных ШДА;

формируют учетную запись УЗ в модифицированном списке доступа ДД из следующих данных:

идентификатор ИЗ,

модифицированный ключ ОКЗ,

модифицированный зашифрованный ключ ШКЗ,

модифицированные зашифрованные данные ШДЗ.