РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2003 131 680** (13) **A**

(51) МПК[7] **H 04 L 9/32, G 06 F 12/14**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2003131680/09, 05.07.2001**

(43) Дата публикации заявки: **27.02.2005 Бюл. № 6**

(85) Дата перевода заявки PCT на национальную фазу: **28.10.2003**

(86) Заявка PCT:
RU 01/00272 (05.07.2001)

(87) Публикация PCT:
WO 03/00563 (16.01.2003)

Адрес для переписки:
129010, Москва, ул. Б.Спасская, 25, стр.3, ООО"Юридическая фирма Городисский и Партнеры", пат.пов. Г.Б. Егоровой

(71) Заявитель(и):
Насыпный Владимир Владимирович (RU),
Гуров Георгий Борисович (RU),
Лобанов Геннадий Харитонович (RU),
Назаров Владимир Васильевич (RU),
Шишов Александр Борисович (RU)

(72) Автор(ы):
Насыпный Владимир Владимирович (RU)

(54) СПОСОБ КОМПЛЕКСНОЙ ЗАЩИТЫ РАСПРЕДЕЛЕННОЙ ОБРАБОТКИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СИСТЕМА ДЛЯ ОСУЩЕСТВЛЕНИЯ СПОСОБА

Формула изобретения

1. Способ комплексной защиты распределенной обработки информации в компьютерных системах, при котором на каждом пользовательском устройстве и на серверах распределенной обработки данных получают доступ к компьютерной системе и формируют систему внутренних и внешних ключей на основе таблиц секретных ключей, полученных из центра сертификации, формирования и распределения ключей, на основе полученных таблиц секретных ключей генерируют в пользовательском устройстве и в сервере распределенной обработки секретные внутренние одноразовые ключи для симметричного режима шифрования при передаче в среде пользовательского устройства и сервера данных, хранении и обработке информации в зашифрованном виде, шифруют вводимые и передаваемые в среде пользовательского устройства и сервера распределенной обработки данные, подлежащие обработке, путем стохастического кодирования с использованием полученных секретных внутренних симметричных одноразовых ключей, направляют с пользовательского устройства в центр сертификации, формирования и распределения ключей запрос на установление соединения с предварительно выбранным сервером распределенной обработки данных для выполнения указанной функции обработки, получают из центра сертификации, формирования и распределения ключей или формируют в пользовательском устройстве и в сервере распределенной обработки открытые ключи для модернизации таблиц секретных ключей для осуществления стохастического кодирования информации, передаваемой от пользовательского устройства в упомянутый сервер распределенной обработки, обработки информации в преобразованном виде и выдачи результата распределенной обработки от упомянутого сервера распределенной обработки в пользовательское устройство, на основе полученных

RU 2003131680 A

RU 2003131680 A

открытых ключей и таблиц секретных ключей генерируют в пользовательском устройстве и в сервере распределенной обработки секретные внешние одноразовые ключи для симметричного режима шифрования, а также осуществляют модификацию таблиц секретных ключей при передаче информации и обработке ее в зашифрованном виде, шифруют передаваемую информацию путем стохастического кодирования в пользовательском устройстве с применением полученных секретных внешних симметричных одноразовых ключей, передают шифрованную путем стохастического кодирования информацию в сервер распределенной обработки, принимают и обрабатывают в сервере распределенной обработки полученную информацию, стохастически кодированную с помощью секретных внешних симметричных одноразовых ключей, в зашифрованном виде после ее дополнительного шифрования с использованием секретных внутренних симметричных одноразовых ключей в соответствии с типом обработки, определяемым по формату упомянутых данных, при этом стохастически кодируют зашифрованную информацию, полученную в результате обработки в сервере распределенной обработки, с использованием секретных внешних симметричных одноразовых ключей, передают стохастически кодированную зашифрованную информацию в пользовательское устройство, принимают стохастически кодированную зашифрованную информацию в пользовательском устройстве и декодируют ее для выдачи пользователю в открытом виде.

2. Способ по п.1, отличающийся тем, что доступ к компьютерной системе и формирование системы внутренних и внешних ключей осуществляют путем ввода в пользовательское устройство носителя данных с записью PIN-кода, пароля, значения хэш-функции пароля, таблицы начального ключа и данных секретных перестановок столбцов и строк для получения секретной таблицы базового ключа и секретной таблицы внешнего ключа.

3. Способ по п.1 или 2, отличающийся тем, что систему ключей формируют в виде набора таблиц секретных базового и внешнего ключей, генерируемых путем секретных перестановок столбцов и строк таблицы начального ключа, которые получают из центра сертификации, формирования и распределения ключей.

4. Способ по любому из пп.1-3, отличающийся тем, что формирование таблиц секретных симметричных внутренних одноразовых ключей для передачи информации отдельно в среде пользовательского устройства и сервера распределенной обработки, шифрования данных, подлежащих обработке, включая таблицы базы данных, Web-страницы и таблицу адресов электронной почты сервера, производят путем перестановок столбцов и строк таблицы базового ключа с использованием секретных перестановок.

5. Способ по любому из пп.1-4, отличающийся тем, что открытые ключи в виде таблиц относительных перестановок формируют в центре сертификации, формирования и распределения ключей, пользовательском устройстве, сервере распределенной обработки путем логического вывода на наборе таблиц секретных перестановок с применением транзитивных зависимостей между элементами строк отдельно для пользовательского устройства и сервера распределенной обработки для приведения их таблиц секретных внешних ключей в симметричное состояние и модификации таблиц секретных ключей.

6. Способ по п.3 или 4, отличающийся тем, что приведение таблиц секретных внешних ключей пользовательского устройства и сервера распределенной обработки в симметричное состояние, а также модификацию таблиц секретных ключей для распределенной обработки зашифрованной информации осуществляют путем использования перестановок и замены столбцов и строк таблиц секретных ключей пользовательского устройства и сервера распределенной обработки с применением открытых ключей.

7. Способ по любому из пп.1-5, отличающийся тем, что генерацию одноразовых ключей осуществляют путем изменения стохастическим образом случайных элементов симметричных ключевых таблиц внешнего или внутреннего ключа для каждого передаваемого блока информации, шифрованной путем стохастического кодирования.

8. Способ по любому из пп.1-5, отличающийся тем, что в процессе шифрования и

RU 2003131680 A

RU 2003131680 A

передачи зашифрованной информации производят периодическую модификацию симметричных ключевых таблиц внешнего и внутреннего ключа в пользовательском устройстве и в сервере распределенной обработки с использованием открытых ключей, формируемых и передаваемых пользовательским устройством и сервером распределенной обработки.

9. Способ по п.1, отличающийся тем, что обработку зашифрованной информации путем выполнения заданных программ в защищенном стохастически преобразованном виде производят в информационно-логическом защищенном вычислительном устройстве с использованием защищенного арифметического процессора, интерфейс которого согласуют по информационным шинам с таблицей секретного внутреннего ключа, а по управляющим шинам передают команды от информационно-логического защищенного вычислительного устройства.

10. Способ по п.9, отличающийся тем, что до или после стохастического преобразования каждой вновь вводимой программы, в информационно-логической защищенной вычислительной системе реализуют антивирусную защиту на основе обнаружения с помощью логического вывода на множестве кодов команд программы вирусных функций в виде цепочек логически связанных кодов команд и уничтожения обнаруженных вирусных функций с обеспечением работоспособности преобразованной программы.

11. Способ по п.1, отличающийся тем, что при определении типа обработки по формату принятой информации как арифметические вычисления выделяют в формате принятых данных зашифрованные операнды и коды арифметических вычислений и передают их в защищенный арифметический процессор для реализации требуемых вычислений в зашифрованном виде.

12. Способ по п.1, отличающийся тем, что при определении типа обработки по формату принятых данных, как поиск и выборка по условиям запроса требуемой информации из зашифрованных таблиц базы данных, выделяют в формате принятой информации зашифрованные данные в условии запроса, по которым после дополнительного шифрования путем сравнения выделяют данные полей зашифрованных таблиц, необходимые для выборки.

13. Способ по п.11 или 12, отличающийся тем, что реализацию указанных проверок соответствия выбираемых данных из зашифрованных таблиц требуемым зашифрованным числовым параметрам или процедур арифметических вычислений с выбранными полями в зашифрованном виде выполняют в защищенном арифметическом процессоре.

14. Способ по п.1, отличающийся тем, что при определении типа обработки по формату принятых данных как поиск и выборка зашифрованных Web-страниц дополнительно шифруют ключевые слова зашифрованного запроса и определяют путем сравнения наличие идентичных ключевых слов в каждой из зашифрованных Web-страниц сервера распределенной обработки.

15. Способ по п.1, отличающийся тем, что при определении типа обработки по формату принятых данных как передача электронной почты принятое зашифрованное сообщение дополнительно шифруют, сравнивают в зашифрованном виде адрес получателя почты с адресами серверов системы и выделяют сервер, содержащий почтовый ящик получателя, которому передается зашифрованная информация.

16. Способ по п.1, отличающийся тем, что формируют значение хэш-функции переданной информации, получают и передают электронную цифровую подпись отправителя информации и осуществляют аутентификацию отправителя и контроль целостности полученной информации, при этом хэш-функцию передаваемой информации в виде случайной комбинации заданной длины формируют с помощью сложения стохастически кодированных блоков в защищенном арифметическом процессоре пользовательского устройства и сервера распределенной обработки.

17. Способ по п.16, отличающийся тем, что электронную цифровую подпись получают путем генерации секретного личного ключа отправителя в виде случайной перестановки строк таблицы секретного внешнего ключа и вычисления открытого ключа, который передают в центр сертификации, формирования и распределения ключей для регистрации

RU 2003131680 A

RU 2003131680 A

личного ключа.

18. Способ по п.16 или 17, отличающийся тем, что аутентификацию отправителя и контроль целостности принятой информации с помощью значения хэш-функции и электронной цифровой подписи секретный личный ключ используют для шифрования хэш-функции переданной информации, а открытый ключ используют для расшифрования принятого значения хэш-функции для сравнения со сформированным в сервере распределенной обработки значением.

19. Система комплексной защиты распределенной обработки информации в компьютерных системах, содержащая центр сертификации, формирования и распределения ключей (1), по меньшей мере одно пользовательское устройство (2) и по меньшей мере один сервер распределенной обработки данных (3), при этом центр сертификации, формирования и распределения ключей (1) содержит подсистему сертификации пользователей (4), подсистему формирования таблиц секретных ключей (5), информационно-логическую защищенную вычислительную систему (6), подсистему формирования носителей данных для сертифицированных пользователей (7), подсистему формирования открытых ключей (8), подсистему аутентификации и проверки целостности информации (9), защищенный арифметический процессор (10), подсистему распределения ключей (11), блок управления защищенной обработкой (12), каждое пользовательское устройство (2) содержит подсистему формирования таблиц секретных ключей (13), внутренний стохастический декодер (14), внутренний стохастический кодер (15), подсистему защищенного доступа (16), защищенный арифметический процессор (19), информационно-логическую защищенную вычислительную систему (20), блок управления защищенной обработкой (21) и приемопередающий блок стохастического преобразования (22), сервер распределенной обработки данных (3) содержит подсистему формирования таблиц секретных ключей (25), приемопередающий блок стохастического преобразования (26), внутреннее устройство стохастического перекодирования (29), блок управления защищенной обработкой (30), подсистему защищенного доступа (31), защищенный арифметический процессор (34), информационно-логическую защищенную вычислительную систему (35) и защищенную базу данных (36), причем в центре сертификации, формирования и распределения ключей (1) информационно-логическая защищенная вычислительная система (6) соединена с подсистемой сертификации пользователей (4), подсистемой формирования таблиц секретных ключей (5), к которой подключена подсистема сертификации пользователей (4), защищенным арифметическим процессором (10), подсистемой формирования открытых ключей (8), подсистемой формирования носителей данных для сертифицированных пользователей (7) и подсистемой распределения ключей (11), с которой соединен блок управления защищенной обработкой (12), соединенный с подсистемой аутентификации и проверки целостности информации (9), в пользовательском устройстве (2) информационно-логическая защищенная вычислительная система (20) соединена с защищенным арифметическим процессором (19), внутренним стохастическим кодером (15), внутренним стохастическим декодером (14) и с приемопередающим блоком стохастического преобразования (22), подсистема защищенного доступа (16) соединена с блоком управления защищенной обработкой (21), соединенным с внутренним стохастическим кодером (15), внутренним стохастическим декодером (14), приемопередающим блоком стохастического преобразования (22), подсистемой формирования таблиц секретных ключей (13) и информационно-логической защищенной вычислительной системой (20), в сервере распределенной обработки данных (3) информационно-логическая защищенная вычислительная система (35) соединена с защищенным арифметическим процессором (34), защищенной базой данных (36), внутренним устройством стохастического перекодирования (29) и блоком управления защищенной обработкой (30), с которым соединены приемопередающий блок стохастического преобразования (26), внутреннее устройство стохастического перекодирования (29), подсистема формирования таблиц секретных ключей (25) и подсистема защищенного доступа (31), при этом подсистема распределения ключей (11)

RU 2003131680 A

RU 2003131680 A

центра сертификации, формирования и распределения ключей (1) соединена соответственно с подсистемами формирования таблиц секретных ключей (13, 25) пользовательского устройства (2) и сервера распределенной обработки данных (3).

20. Система по п.19, отличающаяся тем, что подсистема защищенного доступа (16) пользовательского устройства (2) содержит подсистему ввода информации с носителя данных (17), соединенную с подсистемой аутентификации и проверки целостности информации (18), соединенной с блоком управления защищенной обработкой (21) пользовательского устройства (2).

21. Система по п.19, отличающаяся тем, что приемопередающий блок стохастического преобразования (22) пользовательского устройства (2) содержит первое и второе устройства стохастического перекодирования (23, 24), причем первое устройство стохастического перекодирования (23) включено в тракт передачи данных от сервера распределенной обработки (3) к информационно-логической защищенной вычислительной системе (20) пользовательского устройства (2), а второе устройство стохастического перекодирования (24) включено в тракт приема данных от информационно-логической защищенной вычислительной системы (20) пользовательского устройства (2) к серверу распределенной обработки (3).

22. Система по п.19 или 21, отличающаяся тем, что приемопередающий блок стохастического преобразования (26) сервера распределенной обработки (3) содержит первое и второе устройства стохастического перекодирования (27, 28), причем первое устройство стохастического перекодирования (27) включено в тракт передачи данных от блока управления защищенной обработкой (30) сервера распределенной обработки (3) к приемопередающему блоку стохастического преобразования (22) пользовательского устройства (2), а второе устройство стохастического перекодирования (28) включено в тракт приема данных от приемопередающего блока стохастического преобразования (22) пользовательского устройства (2).

23. Система по любому из пп.19-22, отличающаяся тем, что подсистема защищенного доступа (31) сервера распределенной обработки (3) содержит подсистему ввода информации с носителя данных (32), соединенную с подсистемой аутентификации и проверки целостности информации (33), соединенную с блоком защищенной обработки (30) сервера распределенной обработки (3).

24. Система по любому из пп.19-23, отличающаяся тем, что защищенная база данных (36) сервера распределенной обработки (3) включает в себя защищенную таблицу адресов электронной почты (37), защищенный массив Web-страниц (38) и защищенные таблицы данных (39).

25. Подсистема формирования открытых ключей для системы комплексной защиты распределенной обработки информации в компьютерных системах, содержащая блок памяти для таблиц секретных перестановок столбцов и строк таблиц секретных ключей (61), блок памяти для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа (62), регистр последовательности транзитивной связи между строками таблиц секретных перестановок (63), блок логического вывода на последовательности транзитивной зависимости (64), блок памяти для таблицы относительной несекретной перестановки столбцов и строк таблицы внешнего ключа (65), регистр открытого ключа (66), входной блок коммутации (67), вход которого является входом ввода исходных данных подсистемы, выходной блок коммутации (68), выход которого является выходом вывода открытого ключа подсистемы, и блок управления (69), при этом выходы блока управления (69) соединены соответственно с входами блока памяти для таблиц секретных перестановок столбцов и строк таблиц секретных ключей (61), блока памяти для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа (62), регистра последовательности транзитивной связи между строками таблиц секретных перестановок (63), регистра открытого ключа (66), входного и выходного блоков коммутации (67, 68), блока логического вывода на последовательности транзитивной зависимости (64), второй и третий входы которого соединены соответственно с выходами блока памяти для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа (62) и регистра

RU 2003131680 A

RU 2003131680 A

последовательности транзитивной связи между строками таблиц секретных перестановок (63), а выход – с входом блока памяти для таблицы относительной несекретной перестановки столбцов и строк таблицы внешнего ключа (65), выход которого соединен с входом регистра открытого ключа (66), выход которого соединен с входом выходного блока коммутации (68), другой вход которого соединен с выходами блока памяти для таблиц секретных перестановок столбцов и строк таблиц секретных ключей (61), соединенного своим входом с выходом входного блока коммутации (67), причем вторые выходы входного блока коммутации (67) и выходного блока коммутации (68) соединены с входом блока управления (69).

26. Стохастический кодер для системы комплексной защиты распределенной обработки информации, содержащий входной регистр перестановки (78), вход которого является входом кодируемых данных стохастического кодера, блок регистров столбцов многоалфавитного кодера (79-1,…,79-n), первым входом соединенный с выходом входного регистра перестановки (78), схему подключения столбцов (80), выходами соединенную со вторыми входами блока регистров столбцов многоалфавитного кодера (79-1,…,79-n), циклический регистр перестановки (81), выходами соединенный с соответствующими входами схемы подключения столбцов (80), блок ключей-инверторов (82-1,…,82-n), выходы которого соединены с соответствующими входами циклического регистра перестановки (81), рекуррентный регистр (83), выходами соединенный с соответствующими входами блока ключей-инверторов (82-1,…,82-n), схему формирования гаммы (84), сумматор по mod 2 (85), входы которого соединены соответственно с выходами блока регистров столбцов многоалфавитного кодера (79-1, ..., 79-n) и схемы формирования гаммы (84), а выход – с входом выходного регистра кодового блока (86), выход которого является выходом кодированных данных стохастического кодера, и блок управления (87), выходы которого соединены соответственно со входами входного регистра перестановки (78), блока регистров столбцов многоалфавитного кодера (79-1, ..., 79-n), схемы подключения столбцов (80), циклического регистра перестановки (81), блока ключей-инверторов (82-1, ..., 82-n), рекуррентного регистра (83), схемы формирования гаммы (84), сумматора по mod 2 (85) и выходного регистра кодового блока (86), при этом блок управления (87), со входом которого соединен дополнительный выход рекуррентного регистра (83), имеет дополнительные вход и выход для соединения с другими блоками управления системы комплексной защиты распределенной обработки информации.

27. Стохастический кодер по п.26, отличающийся тем, что схема формирования гаммы (84) содержит блок регистров столбцов таблицы формирования гаммы (88-1, ..., 88-n), схему подключения столбцов (89), выходами соединенную со входами блока регистров столбцов таблицы формирования гаммы (88-1, ..., 88-n), циклический регистр перестановки (90), выходами соединенный с соответствующими входами схемы подключения столбцов (89), блок ключей-инверторов (91-1, ..., 91-n), выходы которого соединены с соответствующими входами циклического регистра перестановки (90), рекуррентный регистр (92), выходами соединенный с соответствующими входами блока ключей-инверторов (91-1, ..., 91-n), регистр исходной гаммы (93), сумматор по mod 2 (94), ключ (95), вход которого соединен с выходом блока регистров столбцов таблицы формирования гаммы (88-1, ..., 88-n), а первый и второй выходы – соответственно со входом сумматора по mod 2 (94) схемы формирования гаммы (84) и со входом сумматора по mod 2 (85) стохастического кодера, и блок управления (96), выходы которого соединены соответственно со входами рекуррентного регистра (92), блока ключей-инверторов (91-1, ..., 91-n), циклического регистра перестановки (90), схемы подключения столбцов (89), блока регистров столбцов таблицы формирования гаммы (88-1, ..., 88-n), ключа (95), сумматора по mod 2 (94), схемы формирования гаммы (84) и регистра исходной гаммы (93), выходом соединенного со входом блока управления (96) схемы формирования гаммы, второй вход которого соединен с дополнительным выходом рекуррентного регистра (92), а третий вход которого соединен с соответствующим выходом блока управления (87) стохастического кодера.

28. Устройство стохастического перекодирования для системы комплексной защиты

RU 2003131680 A

RU 2003131680 A

распределенной обработки информации, содержащее входной регистр кодового блока (97), первую ступень стохастического преобразования (98), вход которой соединен с выходом входного регистра кодового блока (97), первый регистр перестановки (99), первый и второй входы которого соединены соответственно с первым и вторым выходами первой ступени стохастического преобразования (98), второй регистр перестановки (100), первые входы которого соединены соответственно с выходами первого регистра перестановок, вторую ступень стохастического преобразования (101), вход которой соединен с выходом второго регистра перестановки (100), а первый выход – со вторым входом второго регистра перестановки (100), и выходной регистр кодового блока (102), вход которого соединен со вторым выходом второй ступени стохастического преобразования (101), при этом каждая из упомянутых ступеней стохастического преобразования (98, 101) содержит блок регистров столбцов многоалфавитного кодера (79-1, ..., 79-n), первый вход которого является входом соответствующей ступени стохастического преобразования, схему подключения столбцов (80), выходами соединенную со вторыми входами блока регистров столбцов многоалфавитного кодера (79-1, ..., 79-n), циклический регистр перестановки (81), выходами соединенный с соответствующими входами схемы подключения столбцов (80), блок ключей-инверторов (82-1, ..., 82-n), выходы которого соединены с соответствующими входами циклического регистра перестановки (81), рекуррентный регистр (83), выходами соединенный с соответствующими входами блока ключей-инверторов (82-1, ..., 82-n), схему формирования гаммы (84), сумматор по mod 2 (85), первый вход которого через ключ (103) соединен с выходом блока регистров столбцов многоалфавитного кодера (79-1, ..., 79-n), а второй вход – с выходом схемы формирования гаммы (84), причем второй выход ключа (103) является вторым выходом соответствующей ступени стохастического преобразования (98, 101), блок управления (87), первый выход которого является первым выходом соответствующей ступени стохастического преобразования (98, 101), а остальные выходы соединены соответственно со входами блока регистров столбцов многоалфавитного кодера (79-1, ..., 79-n), схемы подключения столбцов (80), циклического регистра перестановки (81), блока ключей-инверторов (82-1, ..., 82-n), рекуррентного регистра (83), дополнительным выходом соединенного с соответствующим входом блока управления (87), схемы формирования гаммы (84), сумматора по mod 2 (85) и ключа (103), при этом блок управления (87) имеет дополнительные вход и выход для соединения с другими блоками управления системы комплексной защиты распределенной обработки информации.

RU 2003131680 A

RU 2003131680 A