РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 259 639** (13) **C2**

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

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

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

(24) Дата начала действия патента: **05.07.2001**

(43) Дата публикации заявки: **27.02.2005**

(45) Опубликовано: **27.08.2005 Бюл. № 24**

(56) Список документов, цитированных в отчете о поиске: **RU 2137185 C1, 10.09.1999.**
RU 2144269 C1, 10.01.2000.
WO 00/01108 A2, 06.01.2000.
RU 95102477 A1, 27.12.1996.
RU 99104428 A, 27.01.2001.
ШЕНДЕРОВИЧ А.М. Прием и воспроизведение цветного изображения в телевизионном приемнике. - М.: Связь, 1970, с.6,7.

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

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

(87) Публикация PCT:
WO 03/005638 (16.01.2003)

Адрес для переписки:
129010, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
Насыпный В.В. (RU)

(73) Патентообладатель(ли):
Насыпный Владимир Владимирович (RU),
Гуров Георгий Борисович (RU),
Лобанов Геннадий Харитонович (RU),
Назаров Владимир Васильевич (RU),
Шишов Александр Борисович (RU)

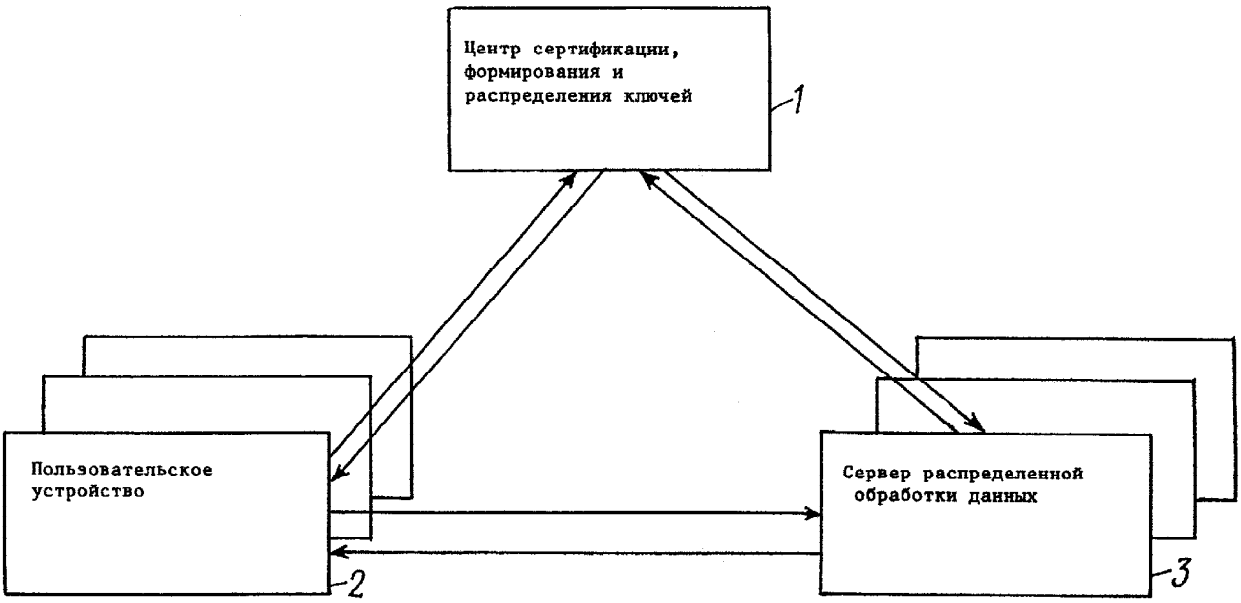
RU 2259639 C2

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

(57) Реферат:

Изобретение относится к средствам защиты информационных систем от несанкционированного доступа. Техническим результатом является возможность формирования сквозного контура защиты распределенной обработки информации. Система комплексной защиты распределенной обработки информации в компьютерных системах содержит центр сертификации, формирования и распределения ключей, по меньшей мере одно пользовательское устройство и по меньшей мере один сервер распределенной обработки данных. Способ описывает работу указанной системы. Подсистема формирования открытых ключей содержит блок памяти для таблиц секретных перестановок столбцов и строк таблиц секретных ключей, блок памяти для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа, регистр последовательности транзитивной связи между строками таблиц секретных перестановок, блок логического вывода на последовательности транзитивной зависимости, блок памяти для таблицы относительной несекретной перестановки столбцов и строк таблицы внешнего ключа, регистр открытого ключа, входной блок коммутации и блок управления. 5 н. и 23 з.п. ф-лы, 14 ил.

RU 2259639 C2



ФИГ. 1

RU 2259639 C2

RU 2259639 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 259 639** (13) **C2**

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

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

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

(24) Effective date for property rights: **05.07.2001**

(43) Application published: **27.02.2005**

(45) Date of publication: **27.08.2005 Bull. 24**

(85) Commencement of national phase: **28.10.2003**

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

(87) PCT publication:
WO 03/005638 (16.01.2003)

Mail address:
129010, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
Nasypnyj V.V. (RU)

(73) Proprietor(s):
Nasypnyj Vladimir Vladimirovich (RU),
Gurov Georgij Borisovich (RU),
Lobanov Gennadij Kharitonovich (RU),
Nazarov Vladimir Vasil'evich (RU),
Shishov Aleksandr Borisovich (RU)

RU 2259639 C2

(54) METHOD FOR COMPLEX PROTECTION OF DISTRIBUTED INFORMATION PROCESSING IN COMPUTER SYSTEMS AND SYSTEM FOR REALIZATION OF SAID METHOD

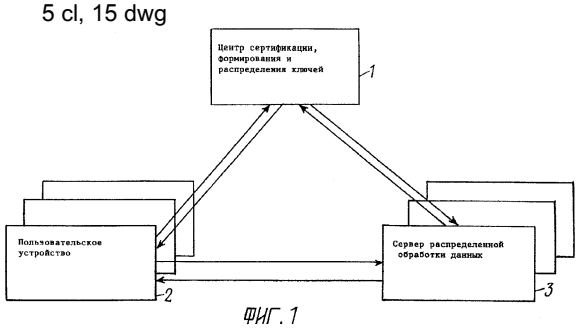
(57) Abstract:

FIELD: computer science.

SUBSTANCE: system has center of certification, forming and distribution of keys, at least one user device and at least one distributed data processing server. Method describes operation of said system. Subsystem for forming open keys contains memory block for tables of secret substitutions of columns and rows of secret keys tables, memory block for table of symmetric substitution of columns and rows of external key table, register for sequence of transitive connection between rows of secret substitutions tables, block for logical output on sequence of transitive dependence, memory block for table of relative non-secret substitution of columns and rows of external key table, open key register, input commutation block and control block.

EFFECT: higher efficiency, broader functional capabilities.

5 cl, 15 dwg



ФИГ. 1

RU 2259639 C2

Область техники

Изобретение относится к области вычислительной техники, информационных систем и средств защиты от несанкционированного доступа.

Предшествующий уровень техники

Для эффективного функционирования информационных систем, основанных на современных компьютерных технологиях и связанных с обработкой и передачей конфиденциальных данных (например, электронная почта, современные платежные системы, поисковые системы), необходимо обеспечить гарантированную защиту процесса распределенной обработки. В настоящее время наиболее защищенным видом распределенной обработки является электронная почта. Известны способы защиты электронной почты (см. международные заявки WO/0049766 от 24.08.2000; WO/9817042 от 23.04. 1998; WO/0001108, от 06.01.2000). Известные способы защиты обеспечивают конфиденциальность передачи информации, электронно-цифровую подпись, идентификацию и аутентификацию отправителя и получателя информации. В способе по заявке WO/0001108 делается попытка обеспечить конфиденциальность адресной части сообщений путем введения анонимных или псевдоанонимных идентификаторов пользователя. Они включают в себя имя, адрес, сведения финансового характера и вводятся с применением посредника. При этом обеспечивается сертификация подлинного и анонимного идентификаторов пользователя. Однако такая система недостаточно надежна, поскольку, во-первых, она не является криптографически стойкой, а во-вторых, существуют участки передачи между пользователем и посредником, где подлинный (истинный) идентификатор передается в открытом виде и может быть перехвачен злоумышленником для взламывания всей системы анонимной идентификации.

Главным недостатком указанных способов является то, что в серверах сети обработка адресной части сообщений производится в открытом виде с использованием незащищенных программ электронной почты, т.е. в исходных кодах команд и данных. Это делает уязвимым к информационным воздействиям как обрабатываемую адресную информацию, так и программы электронной почты. В результате может произойти заражение программ вирусом, искажение алгоритма их работы или адресной части сообщения, а также несанкционированная замена (или изменение) адреса сообщения.

Проблема защиты процесса обработки информации существует и в других системах распределенной обработки информации, например, в системах электронных платежей при удаленном доступе к базам данных для выборки сообщений по запросу пользователя, информационно-поисковых системах, где арифметические вычисления и обработка информации производятся в открытом виде. Поэтому одной из наиболее актуальных задач обеспечения безопасности таких систем является защита от несанкционированного доступа, а также других информационных воздействий (вирусов, программных закладок) на процессы обработки сообщений и выполнения программ в самих компьютерах (пользовательских устройствах и серверах сети).

Известен способ комплексной защиты процесса обработки информации в ЭВМ от несанкционированного доступа, программных закладок и вирусов (см. патент РФ № 2137185 от 09.01.98), который обеспечивает возможность обработки программ и данных в компьютере в стохастически кодированном, защищенном виде с изменением кодов команд, данных и алгоритма в ходе эксплуатации программ. Известный способ реализует два уровня защиты: логический - на основе стохастического преобразования алгоритма (управляющей структуры) программы, и физический, реализуемый за счет стохастического кодирования машинных команд. Вследствие такого преобразования закладки и вирусы не могут найти точку входа в программу для воздействия на нее. Известный способ позволяет обрабатывать числовую информацию в защищенном виде в процессе выполнения арифметических вычислений. Однако этот способ не обеспечивает комплексной защиты всего контура распределенной обработки информации, включающей функции передачи по каналам связи. Это обусловлено тем, что при реализации способа с использованием существующих средств криптографической защиты передачи данных в

интерфейсах подключения защищенных линий связи к компьютеру происходит дешифрирование информации, вследствие чего обработка информации перед стохастическим кодированием будет производиться в открытом виде. Образовавшееся «окно» разрывает единый контур защиты распределенной обработки информации и является возможным источником ее «утечки» путем несанкционированного доступа к ней, в том числе с использованием побочных электромагнитных излучений.

Раскрытие изобретения

Задачей изобретения является создание способа и системы комплексной защиты распределенной обработки информации, обеспечивающих формирование сквозного контура защиты распределенной обработки информации, комплексную гарантированную защиту процесса распределенной обработки информации от несанкционированного доступа и повышение скорости передачи кодированных сообщений.

Указанный технический результат достигается тем, что в способе комплексной защиты распределенной обработки информации в компьютерных системах 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, включая информацию в базе данных, Web-страницы и таблицу адресов электронной почты сервера распределенной обработки, 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 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 ее обработке 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, обрабатывают полученную информацию, стохастически кодированную с помощью секретных внешних симметричных ключей в зашифрованном виде после ее дополнительного шифрования с использованием секретных внутренних одноразовых симметричных 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.

При этом 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.

Систему ключей предпочтительно 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.

Кроме того, формирование таблиц секретных внутренних одноразовых ключей для передачи информации отдельно в среде пользовательского устройства и сервера распределенной обработки, шифрования данных, включая таблицы базы данных, Web-страницы и таблицу адресов электронной почты сервера, производят путем перестановок столбцов и строк таблиц базового ключа с использованием секретных перестановок.

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, причем 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.

При этом генерацию одноразовых ключей предпочтительно осуществляют путем изменения стохастическим образом случайных элементов симметричных ключевых таблиц внешнего или внутреннего ключа для каждого передаваемого блока информации, шифрованной путем стохастического кодирования.

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

Кроме того, 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, причем 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.

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, а при определении типа обработки как поиск и выборка по условиям запроса требуемой информации из зашифрованных таблиц базы данных выделяют зашифрованные данные, по которым после дополнительного шифрования путем сравнения выделяют данные полей зашифрованных таблиц, необходимые для выборки, при этом реализацию 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.

Кроме того, при определении типа обработки 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, а при определении типа обработки как передача электронной почты принятое зашифрованное сообщение дополнительно шифруют и сравнивают в зашифрованном виде адрес получателя почты с адресами серверов системы и выделяют сервер, содержащий почтовый ящик получателя, которому передается зашифрованная информация.

Кроме того, 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, а 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 личного ключа, причем 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.

Указанный технический результат также достигается тем, что система комплексной защиты распределенной обработки информации в компьютерных системах содержит центр сертификации, формирования и распределения ключей, по меньшей мере одно пользовательское устройство и по меньшей мере один сервер распределенной обработки данных, при этом центр сертификации, формирования и распределения ключей содержит подсистему сертификации пользователей, подсистему формирования таблиц секретных ключей, информационно-логическую защищенную вычислительную систему, подсистему формирования носителей данных для сертифицированных пользователей, подсистему формирования открытых ключей, подсистему аутентификации и проверки целостности информации, защищенный арифметический процессор, подсистему распределения ключей, блок управления защищенной обработкой, каждое пользовательское устройство содержит подсистему формирования таблиц секретных ключей, внутренний стохастический декодер, внутренний стохастический кодер, подсистему защищенного доступа, защищенный арифметический процессор, информационно-логическую защищенную вычислительную систему, блок управления защищенной обработкой и приемопередающий блок стохастического преобразования, сервер распределенной обработки данных содержит подсистему формирования таблиц секретных ключей, приемопередающий блок стохастического преобразования, внутреннее устройство стохастического перекодирования, блок управления защищенной обработкой, подсистему защищенного доступа, защищенный арифметический процессор, информационно-логическую защищенную вычислительную систему и защищенную базу данных, причем в центре сертификации, формирования и распределения ключей информационно-логическая

защищенная вычислительная система соединена с подсистемой сертификации пользователей, подсистемой формирования таблиц секретных ключей, к которой подключена подсистема сертификации пользователей, защищенным арифметическим процессором, подсистемой формирования открытых ключей, подсистемой формирования носителей данных для сертифицированных пользователей и подсистемой распределения ключей, с которой соединен блок управления защищенной обработкой, соединенный с подсистемой аутентификации и проверки целостности информации, в пользовательском устройстве информационно-логическая защищенная вычислительная система соединена с защищенным арифметическим процессором, внутренним стохастическим кодером, внутренним стохастическим декодером и с приемопередающим блоком стохастического преобразования, подсистема защищенного доступа соединена с блоком управления защищенной обработкой, соединенным с внутренним стохастическим кодером, внутренним стохастическим декодером, приемопередающим блоком стохастического преобразования, подсистемой формирования таблиц секретных ключей и информационно-логической защищенной вычислительной системой, в сервере распределенной обработки данных информационно-логическая защищенная вычислительная система соединена с защищенным арифметическим процессором, защищенной базой данных, внутренним устройством стохастического перекодирования и блоком управления защищенной обработкой, с которым соединены приемопередающий блок стохастического преобразования, внутреннее устройство стохастического перекодирования, подсистема формирования таблиц секретных ключей и подсистема защищенного доступа, при этом подсистема распределения ключей центра сертификации, формирования и распределения ключей соединена соответственно с подсистемами формирования таблиц секретных ключей пользовательского устройства и сервера распределенной обработки данных.

При этом подсистема защищенного доступа пользовательского устройства содержит подсистему ввода информации с носителя данных, соединенную с подсистемой аутентификации и проверки целостности информации, соединенной с блоком управления защищенной обработкой пользовательского устройства.

Приемопередающий блок стохастического преобразования пользовательского устройства содержит первое и второе устройства стохастического перекодирования, причем первое устройство стохастического перекодирования включено в тракт передачи данных от сервера распределенной обработки к информационно-логической защищенной вычислительной системе пользовательского устройства, а второе устройство стохастического перекодирования включено в тракт приема данных от информационно-логической защищенной вычислительной системы пользовательского устройства к серверу распределенной обработки.

Кроме того, приемопередающий блок стохастического преобразования сервера распределенной обработки содержит первое и второе устройства стохастического перекодирования, причем первое устройство стохастического перекодирования включено в тракт передачи данных от блока управления защищенной обработкой сервера распределенной обработки к приемопередающему блоку стохастического преобразования пользовательского устройства, а второе устройство стохастического перекодирования включено в тракт приема данных от приемопередающего блока стохастического преобразования пользовательского устройства.

Кроме того, подсистема защищенного доступа сервера распределенной обработки содержит подсистему ввода информации с носителя данных, соединенную с подсистемой аутентификации и проверки целостности информации, соединенную с блоком защищенной обработки сервера распределенной обработки.

При этом защищенная база данных сервера распределенной обработки включает в себя защищенную таблицу адресов электронной почты, защищенный массив Web-страниц и защищенные таблицы данных.

Кроме того, указанный технический результат достигается тем, что подсистема формирования открытых ключей для системы комплексной защиты распределенной

обработки информации в компьютерных системах содержит блок памяти для таблиц секретных перестановок столбцов и строк таблиц секретных ключей, блок памяти для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа, регистр последовательности транзитивной связи между строками таблиц секретных перестановок, блок логического вывода на последовательности транзитивной зависимости, блок памяти для таблицы относительной несекретной перестановки столбцов и строк таблицы внешнего ключа, регистр открытого ключа, входной блок коммутации, вход которого является входом ввода исходных данных подсистемы, выходной блок коммутации, выход которого является выходом вывода открытого ключа подсистемы, и блок управления, при этом выходы блока управления соединены соответственно с входами блока памяти для таблиц секретных перестановок столбцов и строк таблиц секретных ключей, блока памяти для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа, регистра последовательности транзитивной связи между строками таблиц секретных перестановок, регистра открытого ключа, входного и выходного блоков коммутации, блока логического вывода на последовательности транзитивной зависимости, второй и третий входы которого соединены соответственно с выходами блока памяти для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа и регистра последовательности транзитивной связи между строками таблиц секретных перестановок, а выход - с входом блока памяти для таблицы относительной несекретной перестановки столбцов и строк таблицы внешнего ключа, выход которого соединен с входом регистра открытого ключа, выход которого соединен с входом выходного блока коммутации, другой вход которого соединен с выходами блока памяти для таблиц секретных перестановок столбцов и строк таблиц секретных ключей, соединенного своим входом с выходом входного блока коммутации, причем вторые выходы входного и выходного блока коммутации соединены с входом блока управления.

Указанный технический результат достигается тем, что стохастический кодер для системы комплексной защиты распределенной обработки информации содержит входной регистр перестановки, вход которого является входом кодируемых данных стохастического кодера, блок регистров столбцов многоалфавитного кодера, первым входом соединенный с выходом входного регистра перестановки, схему подключения столбцов, выходами соединенную со вторыми входами блока регистров столбцов многоалфавитного кодера, циклический регистр перестановки, выходами соединенный с соответствующими входами схемы подключения столбцов, блок ключей-инверторов, выходы которого соединены с соответствующими входами циклического регистра перестановки, рекуррентный регистр, выходами соединенный с соответствующими входами блока ключей-инверторов, схему формирования гаммы, сумматор по mod 2, входы которого соединены соответственно с выходами блока регистров столбцов многоалфавитного кодера и схемы формирования гаммы, а выход - с входом выходного регистра кодового блока, выход которого является выходом кодированных данных стохастического кодера, и блок управления, выходы которого соединены соответственно с входами входного регистра перестановки, блока регистров столбцов многоалфавитного кодера, схемы подключения столбцов, циклического регистра перестановки, блока ключей-инверторов, рекуррентного регистра, схемы формирования гаммы, сумматора по mod 2 и выходного регистра кодового блока, при этом блок управления, с которым соединен дополнительный выход рекуррентного регистра, имеет дополнительные вход и выход для соединения с другими блоками управления системы комплексной защиты распределенной обработки информации.

При этом схема формирования гаммы содержит блок регистров столбцов таблицы формирования гаммы, схему подключения столбцов, выходами соединенную со входами блока регистров столбцов таблицы формирования гаммы, циклический регистр перестановки, выходами соединенный с соответствующими входами схемы подключения столбцов, блок ключей-инверторов, выходы которого соединены с соответствующими входами циклического регистра перестановки, рекуррентный регистр, выходом соединенный с соответствующими входами блока ключей-инверторов, регистр исходной

гаммы, сумматор по mod 2, ключ, вход которого соединен с выходом блока регистров столбцов таблицы формирования гаммы, а первый и второй выходы - соответственно со входом сумматора по mod 2 схемы формирования гаммы и с входом сумматора по mod 2 стохастического кодера, и блок управления, выходы которого соединены соответственно с входами рекуррентного регистра, блока ключей-инверторов, циклического регистра перестановки, схемы подключения столбцов, блока регистров столбцов таблицы формирования гаммы, ключа, сумматора по mod 2 схемы формирования гаммы и регистра исходной гаммы, выходом соединенного со входом блока управления схемы формирования гаммы, со вторым входом которого соединен дополнительный выход рекуррентного регистра, а третий вход которого соединен с соответствующим выходом блока управления стохастического кодера. Кроме того, указанный технический результат достигается тем, что устройство стохастического перекодирования для системы комплексной защиты распределенной обработки информации содержит входной регистр кодового блока, первую ступень стохастического преобразования, вход которой соединен с выходом входного регистра кодового блока, первый регистр перестановки, первый и второй входы которого соединены соответственно с первым и вторым выходами первой ступени стохастического преобразования, второй регистр перестановки, первые входы которого соединены соответственно с выходами первого регистра перестановок, вторую ступень стохастического преобразования, вход которой соединен с выходом второго регистра перестановки, а первый выход - со вторым входом второго регистра перестановки, и выходной регистр кодового блока, вход которого соединен со вторым выходом второй ступени стохастического преобразования, при этом каждая из упомянутых ступеней стохастического преобразования содержит блок регистров столбцов многоалфавитного кодера, первый вход которого является входом соответствующей ступени стохастического преобразования, схему подключения столбцов, выходами соединенную со вторыми входами блока регистров столбцов многоалфавитного кодера, циклический регистр перестановки, выходами соединенный с соответствующими входами схемы подключения столбцов, блок ключей-инверторов, выходы которого соединены с соответствующими входами циклического регистра перестановки, рекуррентный регистр, выходами соединенный с соответствующими входами блока ключей-инверторов, схему формирования гаммы, сумматор по mod 2, первый вход которого через ключ соединен с выходом блока регистров столбцов многоалфавитного кодера, а второй вход - с выходом схемы формирования гаммы, причем второй выход ключа является вторым выходом соответствующей ступени стохастического преобразования, блок управления, первый выход которого является первым выходом соответствующей ступени стохастического преобразования, а остальные выходы соединены соответственно с входами блока регистров столбцов многоалфавитного кодера, схемы подключения столбцов, циклического регистра перестановки, блока ключей-инверторов, рекуррентного регистра, дополнительным выходом соединенного с соответствующим входом блока управления, схемы формирования гаммы, сумматора по mod 2 и ключа, при этом блок управления имеет дополнительные вход и выход для соединения с другими блоками управления системы комплексной защиты распределенной обработки информации.

Краткое описание чертежей

Изобретение поясняется на примерах его осуществления, иллюстрируемых чертежами, на которых представлено следующее:

фиг.1- обобщенная блок-схема системы комплексной защиты распределенной обработки информации в компьютерных системах;

фиг.2 - блок-схема центра сертификации, формирования и распределения ключей;

фиг.3 - блок- схема пользовательского устройства;

фиг.4 - блок-схема сервера распределенной обработки данных;

фиг.5 - блок-схема подсистемы формирования таблиц секретных ключей, используемой в центре сертификации, формирования и распределения ключей;

фиг.6 - блок-схема подсистемы формирования таблиц секретных ключей, используемой

в пользовательском устройстве и в сервере распределенной обработки информации;

фиг.7 - блок-схема подсистемы формирования открытых ключей, используемой в центре сертификации, формирования и распределения ключей;

фиг.8 - блок-схема подсистемы аутентификации и проверки целостности информации, используемой в центре сертификации, формирования и распределения ключей, пользовательских устройствах и в серверах распределенной обработки;

фиг.9 - блок-схема стохастического кодера, используемого в пользовательских устройствах и в подсистемах аутентификации и проверки целостности информации центра сертификации, формирования и распределения ключей, пользовательских устройств и серверов распределенной обработки;

фиг.10 - блок-схема схемы формирования гаммы для использования в стохастическом кодере по фиг.9;

фиг.11А, 11Б - устройство стохастического перекодирования, используемое в пользовательских устройствах и в серверах распределенной обработки;

фиг.12 - таблицы центра сертификации, формирования и распределения ключей;

фиг.13 - схематичное представление процесса формирования открытых ключей для пользователей в центре сертификации, формирования и распределения ключей;

фиг.14 - схематичное представление процедуры распределения ключей.

Предпочтительные варианты осуществления изобретения

Как показано на фиг.1, система комплексной защиты распределенной обработки информации в компьютерных системах содержит центр 1 сертификации, формирования и распределения ключей, по меньшей мере одно пользовательское устройство 2 и по меньшей мере один сервер 3 распределенной обработки данных. Центр 1 сертификации, формирования и распределения ключей (фиг.2) содержит подсистему 4 сертификации пользователей, подсистему 5 формирования таблиц секретных ключей, информационно-логическую защищенную вычислительную систему 6, подсистему 7 формирования носителей для сертифицированных пользователей, подсистему 8 формирования открытых ключей, подсистему 9 аутентификации и проверки целостности информации, защищенный арифметический процессор 10, подсистему 11 распределения ключей и блок управления 12 защищенной обработкой.

Каждое пользовательское устройство 2 (фиг.3) содержит подсистему 13 формирования таблиц секретных ключей, внутренний стохастический декодер 14, внутренний стохастический кодер 15, подсистему 16 защищенного доступа, включающую в себя подсистему 17 ввода информации с носителя данных и подсистему 18 аутентификации и проверки целостности информации, защищенный арифметический процессор 19, информационно-логическую защищенную вычислительную систему 20, блок управления 21 защищенной обработкой и приемопередающий блок 22 стохастического преобразования, включающий в себя первое и второе устройства 23, 24 стохастического перекодирования информации.

Сервер 3 распределенной обработки данных (фиг.4) содержит подсистему 25 формирования таблиц секретных ключей, приемопередающий блок 26 стохастического преобразования, включающий в себя первое и второе устройства 27, 28 стохастического перекодирования информации, внутреннее устройство 29 стохастического перекодирования, блок управления 30 защищенной обработкой, подсистему 31 защищенного доступа, включающую в себя подсистему 32 ввода информации с носителя данных и подсистему 33 аутентификации и проверки целостности информации, защищенный арифметический процессор 34, информационно-логическую защищенную вычислительную систему 35 и защищенную базу данных 36, включающую в себя защищенную таблицу 37 адресов электронной почты, защищенные массивы Web-страниц 38 и защищенные таблицы данных 39.

В центре 1 сертификации, формирования и распределения ключей (фиг.2) информационно-логическая защищенная вычислительная система 6 соединена с подсистемой 4 сертификации пользователей, соединенной с подсистемой 5 формирования

таблиц секретных ключей, защищенным арифметическим процессором 10, подсистемой 5 формирования таблиц секретных ключей, подсистемой 8 формирования открытых ключей, подсистемой 7 формирования носителей данных для сертифицированных пользователей и подсистемой 11 распределения ключей, с которой соединен блок управления 12 защищенной обработкой, соединенный с подсистемой 9 аутентификации и проверки целостности информации.

В пользовательском устройстве 2 (фиг.3) информационно-логическая защищенная вычислительная система 20 соединена с защищенным арифметическим процессором 19, внутренним стохастическим кодером 15, внутренним стохастическим декодером 14, первым и вторым устройствами 23, 24 стохастического перекодирования информации и блоком управления 21 защищенной обработкой, с которым соединены внутренний стохастический кодер 15, внутренний стохастический декодер 14, первое и второе устройства 23, 24 стохастического перекодирования информации, подсистема 13 формирования таблиц секретных ключей и подсистема 18 аутентификации и проверки целостности информации, с которой соединена подсистема 17 ввода информации с носителя данных.

В сервере 3 распределенной обработки данных (фиг.4) информационно-логическая защищенная вычислительная система 35 соединена с защищенным арифметическим процессором 34, защищенной базой данных 36, включающей в себя защищенную таблицу 37 адресов электронной почты, защищенные массивы 38 Web-страниц и защищенные таблицы 39 данных, с блоком управления 30 защищенной обработкой, с которым соединены первое и второе устройства 27, 28 стохастического перекодирования, внутреннее устройство 29 стохастического перекодирования, подсистема 25 формирования таблиц секретных ключей и подсистема 31 защищенного доступа, включающая в себя подсистему 33 аутентификации и проверки целостности информации, с которой соединена подсистема 32 ввода информации с носителя данных. При этом подсистема 11 распределения ключей центра сертификации, формирования и распределения ключей соединена соответственно с подсистемами 25 и 13 формирования таблиц секретных ключей сервера 3 распределенной обработки данных и пользовательского устройства 2, а первое и второе устройства 27, 28 стохастического перекодирования информации сервера 3 распределенной обработки соединены соответственно с первым и вторым устройствами 23, 24 стохастического перекодирования информации пользовательского устройства 2.

На фиг.5 представлена подсистема 5 формирования таблиц секретных ключей центра 1 сертификации, формирования и распределения ключей, содержащая блок памяти 40 таблицы главного ключа, блок памяти 41 таблиц начальных ключей, блок памяти 42 таблиц распределения ключей, датчик 43 случайных чисел со схемой выбора 44 комбинаций, регистр 45 перестановки столбцов, регистр 46 перестановки строк, блок коммутации 47, подключенный к выходам блока памяти 40 таблицы главного ключа и регистров 45, 46, и блок 48 управления, соединенный с вышеуказанными элементами 40-47.

На фиг.6 представлена подсистема 13, 25 формирования таблиц секретных ключей, используемая в сервере 3 распределенной обработки и в пользовательском устройстве 2. Подсистема 13, 25 формирования таблиц секретных ключей содержит блоки памяти 49, 50, 51, 52 таблиц начального, базового, внешнего и внутреннего ключа, датчик 53 случайных чисел со схемой выбора 54 комбинаций, регистры 55, 56, 57, 58 перестановки столбцов и строк соответственно базового и внешнего ключей, блок коммутации 59, соединенный с выходами блока памяти 49 таблицы начального ключа и вышеупомянутых регистров 55, 56, 57, 58, и блок управления 60, подключенный к вышеуказанным элементам 49-59.

На фиг.7 представлена подсистема 8 формирования открытых ключей центра 1 сертификации, формирования и распределения ключей, содержащая блок памяти 61 для таблиц секретных перестановок столбцов и строк таблиц секретных ключей, блок памяти 62 для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа, регистр 63 последовательности транзитивной связи между строками таблиц секретных перестановок, блок 64 логического вывода на последовательности транзитивной зависимости, блок памяти 65 для таблицы относительной несекретной перестановки

столбцов и строк таблицы внешнего ключа, регистр 66 открытого ключа, входной и выходной блоки 67, 68 коммутации и блок управления 69, выходы которого соединены соответственно с входами упомянутых блоков памяти 61 и 62, регистров 63 и 66, входного и выходного блоков 67, 68 коммутации и блока 64 логического вывода на последовательности транзитивной зависимости, второй и третий входы которого соединены соответственно с выходами блока памяти 62 для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа и регистра 63 последовательности транзитивной связи между строками таблиц секретных перестановок, а выход - с входом блока памяти 65 для таблицы относительной несекретной перестановки столбцов и строк таблицы внешнего ключа, выход которого соединен с входом регистра 66 открытого ключа, подключенного к входу выходного блока 68 коммутации, другой вход которого соединен с выходами блока памяти 61 для таблиц секретных перестановок столбцов и строк таблиц секретных ключей, соединенного своим входом с выходом входного блока коммутации 67.

На фиг.8 представлена подсистема 9 (18, 23) аутентификации и проверки целостности информации, используемая в описанных выше центре 1 сертификации, формирования и распределения ключей, пользовательских устройствах 2 и серверах 3 распределенной обработки. Подсистема аутентификации и проверки целостности информации содержит регистры 70, 71, 72 соответственно пароля, PIN-кода и секретного личного ключа, связанные с блоком коммутации 73, внешний стохастический кодер 74, соединенный с блоком памяти 75 столбцов перекодирования символов кодового блока в числовой код, и схему сравнения 76 значений хэш-функции, связанную с блоком управления 77, соединенным с упомянутыми регистрами 70, 71, 72, с блоком коммутации 73 и с внешним стохастическим кодером 74.

На фиг.9 представлен стохастический кодер 15 пользовательского устройства 2, содержащий входной регистр 78 перестановки, вход которого является входом кодируемых данных стохастического кодера, блок регистров 79-1, 79-2,...,79-n столбцов многоалфавитного кодера, первым входом соединенный с выходом входного регистра 78 перестановки, схему подключения столбцов 80, выходами соединенную со вторыми входами блока регистров 79-1, 79-2,..., 79-n столбцов многоалфавитного кодера, циклический регистр 81 перестановки, выходами соединенный с соответствующими входами схемы 80 подключения столбцов, блок ключей-инверторов 82-1, 82-2,..., 82-n, выходы которого соединены с соответствующими входами циклического регистра 81 перестановки, рекуррентный регистр 83, выходами соединенный с соответствующими входами блока ключей-инверторов 82-1, 82-2,...,82-n, схему 84 формирования гаммы, сумматор по mod 2 85, входы которого соединены соответственно с выходами блока регистров 79-1, 79-2,..., 79-n столбцов многоалфавитного кодера и схемы 84 формирования гаммы, а выход - с входом выходного регистра 86 кодового блока, выход которого является выходом кодированных данных стохастического кодера, и блок управления 87, выходы которого соединены соответственно с входами входного регистра 78 перестановки, рекуррентного регистра 83, блока ключей-инверторов 82-1,82-2,..., 82-n, циклического регистра 81 перестановки, схемы 80 подключения столбцов, блока регистров 79-1, 79-2,...,79-n столбцов многоалфавитного кодера, схемы 84 формирования гаммы, сумматора по mod 2 85 и выходного регистра 86 кодового блока, при этом блок управления 87, с соответствующим входом которого соединен дополнительный выход рекуррентного регистра, имеет дополнительные вход и выход для связи с другими блоками управления системы комплексной защиты распределенной обработки информации.

На фиг.10 показана схема 84 формирования гаммы, входящая в состав стохастического кодера 15, содержащая блок регистров 88-1, 88-2,..., 88-n столбцов таблицы формирования гаммы, схему 89 подключения столбцов, выходами соединенную с входами блока регистров 88-1, 88-2,..., 88-n столбцов таблицы формирования гаммы, циклический регистр 90 перестановки, выходами соединенный с соответствующими входами схемы 89 подключения столбцов, блок ключей-инверторов 91-1, 91-2,..., 91-n, выходы которого соединены с соответствующими входами циклического регистра 90 перестановки,

рекуррентный регистр 92, выходами соединенный с соответствующими входами блока ключей-инверторов 91-1, 91-2,..., 91-n, регистр 93 исходной гаммы, сумматор по mod 2 94, ключ 95, вход которого соединен с выходом блока регистров 88-1, 88-2,..., 88-n столбцов таблицы формирования гаммы, а первый и второй выходы - соответственно со входом сумматора по mod 2 94 схемы формирования гаммы и со входом сумматора по mod 2 85 стохастического кодера 15 (фиг.9), и блок управления 96, выходы которого соединены соответственно со входами рекуррентного регистра 92, блока ключей-инверторов 91-1, 91-2,..., 91-n, циклического регистра 90 перестановки, схемы подключения столбцов 89, блока регистров 88-1, 88-2,..., 88-n столбцов таблицы формирования гаммы, ключа 95, сумматора по mod 2 94 и регистра 93 исходной гаммы, выходом соединенного с входом блока управления 96, второй вход которого соединен с дополнительным выходом рекуррентного регистра, а третий вход которого соединен с соответствующим выходом блока управления 87 стохастического кодера 15.

Стохастический декодер 14 (фиг.3) выполнен аналогично стохастическому кодеру 15, схема которого представлена на фиг.9. Единственное различие заключается в том, что направление прохождения обрабатываемого сигнала в схеме декодера изменено на обратное по сравнению со схемой кодера (фиг.9). Таким образом на блок 86 (выходной регистр кодового блока на фиг.9) в схеме стохастического декодера будут подаваться входные декодируемые данные, а с блока 78 (входной регистр перестановки на фиг.9) будут выдаваться выходные декодированные данные.

На фиг.11А, 11Б показано устройство стохастического перекодирования (23, 24 на фиг.3, 27, 28 на фиг.4), входящее в состав пользовательских устройств 2 и серверов 3 распределенной обработки. Устройство стохастического перекодирования содержит последовательно соединенные входной регистр 97 кодового блока, первую ступень 98 стохастического преобразования, первый и второй регистры 99, 100 перестановки, вторую ступень 101 стохастического преобразования и выходной регистр 102 кодового блока. Первая и вторая ступени 98, 101 имеют идентичную структуру, практически совпадающую со структурой стохастического кодера 15 (см. элементы 79, 80, 81, 82, 83, 84, 85, 87 на фиг.9). По существу различие заключается во введении ключа 103 между выходом блока регистров 79-1, 79-2, 79-n и входом сумматора по mod 2 85, причем выход ключа 103 является выходом соответствующей ступени стохастического преобразования.

На фиг.12 показаны таблицы центра сертификации, формирования и распределения ключей.

Фиг.13 иллюстрирует процесс формирования открытых ключей для пользователей в центре сертификации, формирования и распределения ключей.

На фиг.14 показаны основные этапы процедуры распределения ключей.

Рассмотрим более подробно реализацию предложенной системы комплексной защиты распределенной обработки информации в компьютерных системах (фиг.1).

Основными задачами центра 1 сертификации формирования и распределения ключей являются подключение пользовательских устройств 2 к системе защиты, их сертификация, формирование и распределение закрытых и открытых ключей между пользовательскими устройствами 2 и серверами 3 распределенной обработки данных. В центре 1 сертификации формируется и хранится главный ключ системы (мастер-ключ), который представляет собой случайно заполненную кодами таблицу. Структура центра 1 сертификации представлена на фиг.2. Сертификация пользовательских устройств 2 и серверов 3 распределенной обработки для подключения к системе защиты производится в подсистеме 4 сертификации пользователей. Формирование таблицы главного ключа производится в подсистеме 5 формирования таблиц секретных ключей.

На основе таблицы главного секретного ключа в подсистеме 5 формирования таблиц секретных ключей путем случайной перестановки ее столбцов и строк формируется множество различных таблиц начальных секретных ключей для пользователей. При этом каждой полученной таблице начального секретного ключа ставится в соответствие примененная перестановка столбцов и строк таблицы главного секретного ключа. Затем в

этой же подсистеме 5 для каждой таблицы начального секретного ключа путем случайных перестановок ее столбцов и строк формируются таблицы базового секретного ключа и внешнего секретного ключа. Каждой полученной таблице ставятся в соответствие использованные случайные перестановки столбцов и строк таблицы начального секретного ключа. Все эти процедуры выполняются под управлением информационно-логической защищенной вычислительной системы 6, программы которой выполняются в защищенном виде. Структура и работа информационно-логической защищенной вычислительной системы 6 описаны в патенте РФ №2137185 от 09.01.98.

Полученные таблицы начального ключа и случайные перестановки столбцов и строк для формирования таблиц базового секретного ключа и внешнего секретного ключа поступают в подсистему 7 формирования носителей для сертифицированных пользователей. В этой подсистеме происходит формирование носителей данных и выдача их пользователям, прошедшим сертификацию для подключения к системе защиты распределенной обработки информации в компьютерных системах.

Ключевые перестановки столбцов и строк, которые применяются при формировании каждой таблицы начального ключа, запоминаются в таблице распределения ключей для пользователей (фиг.12). Кроме этого в таблицу записываются полученные от датчика случайных чисел в подсистеме 9 аутентификации и проверки целостности информации пользователя значения PIN-кода и пароля. По комбинации пароля и PIN-кода вычисляется значение его хэш-функции, порядок реализации которой описан ниже. При сертификации пользователя в таблицу также заносятся его паспортные данные. После этого для каждого пользователя в подсистеме 7 формирования носителей для сертификационных пользователей формируется носитель данных - смарт-карта, копия которой хранится в центре сертификации. Она содержит полную таблицу начального ключа, а также набор секретных ключей-перестановок для таблиц базового и внешнего ключей пользователя. Кроме этого в смарт-карту записывается PIN-код и значение хэш-функции пароля данного пользователя (фиг.12). Полученная смарт-карта выдается пользователю для ввода в его компьютер (пользовательское устройство 2 или сервер 3 распределенной обработки).

Для формирования системы ключей пользователь вводит в компьютер информацию со смарт-карты, полученной в центре 1 сертификации, формирования и распределения ключей. После этого в компьютере производится формирование таблицы базового ключа на основе указанных в смарт-карте ключей-перестановок столбцов и строк. Затем с использованием соответствующих перестановок формируется таблица внешнего ключа и кодовая таблица защищенного арифметического процессора 10. Структура и функционирование защищенного арифметического процессора 10 описаны в работе: Насыпный В.В. «Защита арифметических вычислений в компьютерных системах», Мир ПК, 1999, №4, с. 73-74. При этом в пользовательском устройстве 2 и сервере 3 распределенной обработки применяются подсистема 13, 25 формирования таблиц секретных ключей и блок управления 21, 30 защищенной обработкой, а также информационно-логическая защищенная вычислительная система 20, 35 (фиг.3, 4).

В результате на экран монитора выдается сообщение «Введите свой личный пароль». После ввода пароля пользователя в подсистему 16 защищенного доступа в подсистеме 18 аутентификации и проверки целостности информации с использованием таблицы базового ключа и защищенного арифметического процессора 19 вычисляется значение хэш-функции пароля, которое сравнивается с аналогичным значением, введенным со смарт-карты. При совпадении сравниваемых значений активизируется блок управления 21 защищенной обработкой, и пользователь получает доступ к его функциям. Если после m-кратного ввода пароля значение его хэш-функции не совпадет со значением, введенным со смарт-карты, система защиты блокируется, смарт-карта аннулируется. Для получения новой смарт-карты пользователь должен обратиться в центр 1 сертификации, формирования и распределения ключей.

При получении доступа к функциям системы защиты по команде пользователя в пользовательском устройстве 2 на основе таблицы начального ключа и секретных

перестановок, введенных со смарт-карты, производится формирование таблиц базового секретного ключа, а затем таблицы внешнего секретного ключа. Полученные таблицы базового секретного ключа подвергают случайным перестановкам столбцов и строк для формирования таблицы внутреннего секретного ключа. Затем копии полученной таблицы внутреннего секретного ключа записываются во внутренний стохастический кодер 15, внутренний стохастический декодер 14, а также в приемопередающий блок 22, включающий в себя первое и второе устройства 23, 24 стохастического перекодирования информации в пользовательском устройстве 2. Описанные процедуры реализуются путем выполнения защищенных программ в информационно-логической защищенной вычислительной системе 20 по командам блока управления 21, 30 защищенной обработкой. После этого блок 21 управления защищенной обработкой производит настройку внутреннего стохастического кодера 15, внутреннего стохастического декодера 14 и обеспечивает готовность внутрикомпьютерной защищенной передачи и обработки информации в пользовательском устройстве 2.

Такие же процедуры по вводу информации со смарт-карты с использованием подсистемы 31 защищенного доступа, включающей подсистему 32 ввода информации с носителя данных и подсистему 33 аутентификации и проверки целостности информации, выполняются в сервере 3 распределенной обработки. После аутентификации пользователя производится запуск блока управления 30 защищенной обработкой, по команде которого в подсистеме 25 формирования таблиц секретных ключей происходит формирование таблиц внешнего секретного ключа и базового секретного ключа. При этом на основе таблицы начального секретного ключа и секретных перестановок, введенных со смарт-карты, производится сначала формирование таблиц базового секретного ключа, а затем таблицы внешнего секретного ключа. Полученные таблицы базового секретного ключа подвергаются случайным перестановкам столбцов и строк для формирования таблицы внутреннего секретного ключа. Затем копии полученной таблицы внутреннего секретного ключа записываются во внутреннее устройство 29 стохастического перекодирования информации, а также в устройства 27, 28 стохастического перекодирования информации приемопередающего блока 26 стохастического преобразования. Описанные процедуры реализуются путем выполнения защищенных программ в информационно-логической защищенной вычислительной системе 35 по командам блока управления 30 защищенной обработкой. После этого по командам блока управления 30 защищенной обработкой, подключенного к информационно-логической защищенной вычислительной системе 35, происходит шифрование таблицы 35 адресов электронной почты, защищенных таблиц данных 39 и защищенных массивов Web-страниц 38. При этом по команде блока управления 36 защищенной обработкой внутреннее устройство 29 стохастического перекодирования переводится в режим внутреннего стохастического кодера, с которым согласуется интерфейс защищенного арифметического процессора 34.

После завершения описанного процесса формирования ключевых таблиц пользователь может обратиться с запросом к центру 1 сертификации, формирования и распределения ключей для организации закрытой связи с требуемым сервером 3 распределенной обработки (другим пользователем). Этому должна предшествовать договоренность об организации такой связи, полученная по открытой связи. По данному запросу центр 1 сертификации обеспечивает формирование и распределение открытых ключей между пользователями для обеспечения закрытой связи. Структура этого процесса показана на фиг.14.

Рассмотрим функции центра 1 сертификации, формирования и распределения ключей, пользовательского устройства 2 (пользователь А) и сервера 3 распределенной обработки (пользователь В) при организации процесса закрытой связи.

Функции центра сертификации, формирования и распределения ключей:

1) проверка полномочий пользователей А и В на установление закрытой связи;

2) формирование открытого ключа для пользовательского устройства 2;

3) формирование открытого ключа для сервера 3 распределенной обработки;

4) выдача открытых ключей по сети связи в пользовательское устройство 2 и сервер 3 распределенной обработки для установления симметричной закрытой связи;

5) после завершения сеанса связи выдача новых открытых ключей для приведения системы связи в асимметричный режим.

Функции пользователей A (B):

1) получение открытого ключа-перестановки;

2) модификация таблицы внешнего ключа для реализации симметричной закрытой связи;

3) формирование таблицы для устройства 23, 24 (27, 28) стохастического перекодирования информации приемопередающего блока 22 (26) стохастического преобразования;

4) формирование таблицы для схемы формирования гаммы устройств стохастического перекодирования 23, 24 (27, 28);

5) начало передачи информации в закрытом режиме.

Проверка полномочий пользователей пользовательского устройства 2 и сервера 3 распределенной обработки на установление открытой связи проводится в подсистеме 4 сертификации пользователей (фиг.2.) по специальным таблицам, определяющим схему разрешенных информационных взаимодействий пользователей системы в закрытом режиме. Если полномочия пользователей на составление закрытой связи подтверждаются, то в центре сертификации, формирования и распределения ключей производится автоматическое формирование открытых ключей для пользовательского устройства 2 и сервера распределенной обработки 3.

Формирование открытых ключей основано на применении однонаправленной функции, использующей относительные перестановки на достаточно длинных комбинациях случайных символов (длина n >100). Как было отмечено выше, в центре 1 сертификации, формирования и распределения ключей хранятся все ключи-перестановки столбцов и строк, позволяющие из таблицы главного ключа сформировать для каждого пользователя таблицы начального, базового и внешнего секретных ключей. После загрузки системы все эти таблицы, включая таблицу внешних секретных ключей, для разных пользователей будут асимметричны. Для того, чтобы организовать закрытую связь между пользователями A и B, необходимо привести их таблицы внешних секретных ключей в идентичное состояние. Это обеспечивается благодаря наличию в центре 1 сертификации всех указанных выше функционально связанных секретных перестановок таблиц (начального, базового и внешнего секретных ключей).

В подсистеме 8 формирования открытых ключей (фиг.2) с помощью логического вывода на последовательности транзитивной связи между строками таблиц секретных перестановок определяются относительные перестановки для пользователей A и B, которые позволяют привести таблицы внешних секретных ключей в симметричное состояние. Указанные относительные перестановки являются открытыми ключами. На их основе пользователи A и B могут перевести таблицы внешних секретных ключей в идентичное состояние для организации симметричной закрытой связи. С этой целью в подсистему 8 формирования открытых ключей (фиг.2) из подсистемы 5 формирования таблиц секретных ключей через информационно-логическую защищенную вычислительную систему 6 передаются данные таблиц секретных перестановок столбцов и строк таблиц секретных ключей (начального, базового и внешнего). Затем на основе этих таблиц формируются последовательности транзитивной связи между строками таблиц секретных перестановок. Далее с использованием логического вывода на последовательности транзитивной зависимости определяются таблицы относительной несекретной перестановки столбцов и строк таблицы внешнего секретного ключа отдельно для пользовательского устройства 2 и сервера 3 распределенной обработки. Полученные таблицы являются открытыми ключами, обеспечивающими перевод таблиц внешних секретных ключей пользовательского устройства 2 и сервера 3 распределенной обработки в симметричное состояние. Полученные открытые ключи поступают в подсистему 11

распределения ключей и доводятся по компьютерной системе до соответствующих пользовательского устройства 2 и сервера 3 распределенной обработки.

При этом функция формирования открытых ключей с использованием относительной перестановки является однонаправленной для любого пользователя системы. Это обусловлено тем, что в центре 1 сертификации, формирования и распределения ключей, имея полную функциональную схему между ключами-перестановками, можно легко вычислить функцию y=f(x). Здесь x - значение начального, базового или внешнего секретного ключа, f - функциональные связи между ними, заданные секретными перестановками, y - относительная несекретная перестановка. Однако по известному значению y, не зная всей схемы функциональных связей между таблицами, нельзя восстановить секретные перестановки, исходную таблицу начального, базового или внешнего секретного ключа. Поскольку соответствующие таблицы секретных перестановок индивидуальны для каждого пользователя, то никто кроме него не сможет построить новую симметричную таблицу внешнего секретного ключа при организации закрытой связи с заданным абонентом по полученному открытому ключу. Тем более никто не сможет вычислить по сформированному ключу исходные значения таблиц начального, базового или внешнего секретных ключей данного пользователя. Это обусловлено тем, что определение указанных перестановок и таблиц связано с полным перебором всех возможных комбинаций на множестве V=n! (для n=100, например, $V>10^{100,}$ что практически нереализуемо). Поэтому функция y=f(x) является односторонней для всех остальных пользователей системы. При этом даже пользователь B, с которым взаимодействует пользователь A, имеющий после обработки открытого ключа идентичный сеансовый внешний секретный ключ, не сможет вскрыть базовый и начальный секретные ключи пользователя A путем обратной перестановки.

На основе полученных открытых ключей в подсистеме 13 и 25 формирования таблиц секретных ключей пользовательского устройства 2 и сервера 3 распределенной обработки создают таблицы симметричных внешних секретных ключей. Эти таблицы записываются в устройства 23, 24 (27, 28) стохастического перекодирования информации приемопередающего блока 22 (26) стохастического преобразования пользовательского устройства 2 (сервера 3 распределенной обработки), обеспечивая тем самым установление закрытой симметричной связи между ними. При этом в устройствах стохастического перекодирования информации 23, 24 (27, 28) происходит необходимое согласование таблиц внешних и внутренних кодов, обеспечивающих замкнутый контур передачи и обработки защищенной информации между пользовательским устройством 2 и сервером 3 распределенной обработки. Этот контур проходит от внутреннего стохастического кодера 15 пользовательского устройства 2 до внутреннего устройства стохастического перекодирования информации 29 сервера распределенной обработки, подключенного к информационно-логической защищенной вычислительной системе 35 и обратно через внутреннее устройство стохастического перекодирования информации 29 к внутреннему стохастическому декодеру 14 пользовательского устройства 2. При этом в процессе передачи на основе стохастического выбора случайных элементов таблиц внутреннего и внешнего секретных ключей реализуется режим одноразового ключа, обеспечивая требуемый гарантированный уровень защиты информации.

После завершения сеанса закрытой связи центр сертификации посылает пользователям A и B открытые ключи-перестановки для генерации асимметричных таблиц исходных внешних секретных ключей.

Таким образом, исходя из разнообразия функций защиты информации (передача и обработка) система ключей является двухуровневой. Первый уровень - это таблицы начального, базового и внешнего секретных ключей. Эти таблицы пользователь вводит в пользовательское устройство 2, сервер 3 распределенной обработки с использованием полученного в центре 1 сертификации, формирования и распределения ключей носителя данных. Указанные таблицы секретных ключей непрерывно (периодически) обновляются с помощью открытых ключей, формируемых центром сертификации, формирования и

распределения ключей. При этом в процессе передачи информации между пользователями A и B реализуется системная функция периодической модификации таблиц секретных внешних ключей, используемых в стохастическом кодере 14 и в схеме 84 формирования гаммы. Эта функция выполняется с использованием открытых ключей, формируемых в пользовательском устройстве 2 и сервере 3 распределенной обработки (пользователи A и B), которые участвуют в обмене закрытой информацией. В процессе обмена закрытой информацией указанная системная функция является по существу одной из базовых процедур обеспечения его надежности и защищенности. При этом выбор периода модификации таблиц секретных внешних ключей в значительной степени влияет на уровень защищенности информации.

Второй уровень системы ключей представляют стохастические одноразовые ключи. Они формируются на основе таблиц внешнего секретного ключа, используемых в стохастическом кодера 14 и схеме 84 формирования гаммы, путем стохастического выбора уникальных комбинаций случайных элементов указанных таблиц. Этому уровню соответствуют локальные функции стохастического кодирования и гаммирования, реализуемые с использованием стохастических одноразовых ключей.

В общем случае надежность и защищенность процесса стохастического кодирования информации при ее передаче зависит как от периодичности реализации системной функции модификации таблиц секретных внешних ключей, так и от эффективности стохастических одноразовых ключей стохастического кодера 14 и схемы 84 формирования гаммы.

В блоке управления 30 защищенной обработкой по формату принятого сообщения определяют тип обработки, которую необходимо выполнить в защищенной информационно-логической вычислительной системе 35 с использованием закрытых данных и стохастически преобразованных программ. Эта обработка может представлять собой передачу электронной почты, арифметические вычисления, поиск и выборку по условию запроса требуемой информации из зашифрованной базы данных 36. Указанные функции выполняются с помощью внутреннего устройства 29 стохастического перекодирования, подключенного к блоку управления 30 защищенной обработкой и информационно-логической защищенной вычислительной системе 35. Порядок реализации данных функций обработки защищенной информации с использованием защищенных стохастически преобразованных программ в информационно-логической защищенной вычислительной системе 35 описан ниже.

В процессе обработки информации с использованием стохастически преобразованных программ и данных в информационно-логической защищенной вычислительной системе 35 обеспечивается их комплексная защита от несанкционированного доступа, программных закладок и вирусов.

При вводе новых программ до или после стохастического преобразования каждой вновь вводимой программы в информационно-логической защищенной вычислительной системе реализуют антивирусную защиту на основе обнаружения вирусных функций с помощью логического вывода на множестве кодов команд программы. При этом сначала производится выделение кодов команд, которые могут использовать вирусы для реализации несанкционированных действий с программами, данными и текстовыми файлами. Затем с помощью логического вывода получают цепочки логически связанных кодов команд, включая указанные выше «вирусные» коды, и определяют целевую функцию каждой такой цепочки. Если эта целевая функция является вирусной, то данная цепочка логически связанных команд относится к вирусным функциям. В этом случае производится ее уничтожение с обеспечением работоспособности преобразованной программы.

Ниже описана работа отдельных подсистем и устройств системы.

Подсистема 4 сертификации пользователей (фиг.2)

Эта подсистема организационного типа содержит типовые устройства ввода/вывода информации, подключенные к подсистеме 5 формирования таблиц секретных ключей. Она обеспечивает ввод паспортных данных пользователей компьютеров при их сертификации

для подключения к системе защиты распределенной обработки информации в компьютерных системах. Состав паспортных данных записывается в таблицы распределения ключей для пользователей (фиг.12), хранящиеся в подсистеме 5 формирования таблиц секретных ключей.

Подсистема 5 формирования таблиц секретных ключей (фиг.5)

Эта подсистема входит в состав центра 1 сертификации, формирования и распределения ключей. Ее назначение заключается в формировании на основе таблицы главного секретного ключа путем случайной перестановки столбцов и строк множества таблиц начальных секретных ключей для сертифицированных пользователей системы. Кроме этого в данной подсистеме формируются таблицы секретных перестановок столбцов и строк, необходимые для получения на основе таблицы начального секретного ключа таблиц базового и внешнего секретных ключей для каждого пользователя (фиг.12). Запуск этой подсистемы производится по командам, поступающим из информационно-логической защищенной вычислительной системы 6. Туда же подается результат обработки, который поступает затем в подсистему 7 формирования носителей для сертифицированных пользователей, а также в подсистему 8 формирования открытых ключей. По поступившим командам производится запуск блока 48 управления этой подсистемы, которая включает датчик 43 случайных чисел. Начинается процесс генерации последовательности случайных чисел, которая поступает в схему выбора 44 комбинаций. Здесь осуществляется выбор n различных случайных чисел, поступающих через блок 48 управления в регистр 45 перестановки столбцов. После этого таким же образом заполняется n различными случайными числами регистр 46 перестановки строк. Далее датчик 43 случайных чисел временно отключается. Начинается процесс формирования таблицы начального секретного ключа путем перестановки столбцов и строк главного секретного ключа с использованием заполненных регистров 45, 46 перестановки столбцов и строк. С этой целью по командам блока 48 управления сначала производится поочередная выборка строк из таблицы главного секретного ключа, запись каждой строки в регистр 45 перестановки столбцов, где в соответствии с записанной случайной последовательностью производится перестановка полей данной i-ой строки. Полученные данные строки через блок коммутации 47, блок 48 управления поступают в блок памяти 41 таблиц начальных секретных ключей и записываются в формируемую таблицу начального секретного ключа для очередного пользователя. При этом номер строки определяется соответствующим i-ым случайным числом, считанным из регистра перестановки строк. В результате после считывания n строк и выполнения описанных перестановок в блоке памяти 41 таблиц начальных секретных ключей будет сформирована таблица начального секретного ключа для очередного пользователя. После этого данная таблица через блок 48 управления поступает в блок памяти таблиц 42 распределения ключей и записывается в соответствующую таблицу распределения ключей для указанного пользователя (фиг.12). Туда же, через блок коммутации 47 и блок 48 управления записываются последовательности секретных перестановок столбцов и строк из соответствующих регистров. После этого блок 48 управления вновь производит включение датчика 43 случайных чисел, который, как было описано выше, обеспечивает случайные перестановки столбцов и строк сначала для формирования таблицы базового секретного ключа, затем - для таблицы внешнего секретного ключа. Полученные секретные перестановки поочередно через блок коммутации 47 и блок 48 управления поступают в блок памяти таблиц 42 распределения ключей и заносятся в таблицу копии смарт-карты очередного пользователя (фиг.12). Туда же записываются таблицы начального секретного ключа и соответствующие секретные перестановки столбцов и строк из соответствующей таблицы распределения ключей для пользователей. После этого по команде блока 48 управления датчик 43 случайных чисел генерирует значения PIN-кода и пароля для данного пользователя. Полученные значения через схему выбора 44 комбинаций и блока 48 управления поступают в блок памяти таблиц начальных ключей и записываются в таблицу распределения ключей для пользователей, формируемую для указанного пользователя

(фиг.12). Оттуда значения PIN-кода и пароля через блок 48 управления и блок коммутации 47 поступают в информационно-логическую защищенную вычислительную систему 6. Далее эти значения через подсистему 11 распределения ключей и блок управления 12 защищенной обработкой поступают в подсистему 9 аутентификации и проверки целостности информации. Здесь по комбинациям PIN-кода и пароля формируются значения хэш-функций пароля, которые обратным порядком выдаются в подсистему формирования таблиц секретных ключей и записываются в указанную таблицу распределения ключей для пользователей. Порядок формирования хэш-функции пароля в подсистеме 9 аутентификации и проверки целостности информации описан ниже. Затем значения PIN-кода и хэш-функции пароля заносятся в таблицу копии смарт-карты для данного пользователя (фиг.12). После этого сформированная копия смарт-карты пользователя через информационно-логическую вычислительную систему 6 поступает в подсистему 7 формирования носителей для сертифицированных пользователей.

Подсистема 7 формирования носителей для сертифицированных пользователей (фиг.3)

В этой подсистеме производится запись полученной копии смарт-карты на соответствующий носитель информации. Полученный носитель (смарт-карта) выдается соответствующему пользователю. При этом ему в устной форме сообщается значение личного пароля.

Подсистема 13, 25 формирования таблиц секретных ключей пользовательского устройства 2 (сервера 3 распределенной обработки)

Данная подсистема включается в работу после ввода смарт-карты в подсистему 17, 32 ввода информации с носителя данных подсистемы 16, 31 защищенного доступа пользовательского устройства 2 и сервера 3 распределенной обработки и аутентификации пользователя с использованием подсистемы 18, 33 аутентификации пользователя и контроля целостности информации. После аутентификации пользователя по команде от блока управления 21, 30 защищенной обработкой через блок коммутации 59 и блок 60 управления в блок памяти 49 таблицы начального ключа поступает считанная со смарт-карты таблица начального ключа данного пользователя. При этом в регистры 55, 56 перестановки столбцов и строк для формирования базового ключа и в регистры 57, 58 перестановки столбцов и строк для формирования внешнего ключа считываются соответствующие числовые последовательности со смарт-карты.

Затем начинается процесс формирования таблицы базового секретного ключа путем перестановки столбцов и строк начального ключа с использованием заполненных регистров 55, 56 перестановки столбцов и строк для формирования таблицы базового секретного ключа. С этой целью по командам блока 60 управления сначала производится поочередная выборка строк из таблицы начального секретного ключа, занесение каждой строки в регистр 55 перестановки столбцов, где в соответствии с записанной случайной последовательностью производится перестановка полей данной i-ой строки. Полученная строка через блок коммутации 65, блок 60 управления поступает в блок памяти 50 таблицы базового ключа. Там она записывается в формируемую таблицу базового секретного ключа для данного пользователя. При этом номер строки определяется соответствующим i-м случайным числом, считанным из регистра 56 перестановки строк. В результате после считывания n строк и выполнения описанных перестановок в блоке памяти 50 таблицы базового ключа будет сформирована таблица базового секретного ключа данного пользователя.

Полученная таблица базового секретного ключа является исходной при формировании таблицы внешнего секретного ключа на основе n различных случайных чисел, записанных в регистры 57, 58 перестановок столбцов и строк для формирования таблицы внешнего секретного ключа. Порядок формирования таблицы внешнего секретного ключа путем перестановки столбцов и строк таблицы базового секретного ключа идентичен описанному выше алгоритму формирования базового ключа. В результате его реализации в блок памяти 51 таблицы внешнего ключа будет записана полученная таблица внешнего секретного ключа данного пользователя.

После этого по команде блока 60 управления запускается датчик 53 случайных чисел. В результате через схему выбора 54 комбинаций и блок 60 управления в регистры 57, 58 перестановки столбцов и строк для формирования таблицы внешнего секретного ключа поступают случайные последовательности, каждая из которых содержит n различных случайных чисел. В данном случае эти случайные последовательности применяются для формирования таблицы внутреннего секретного ключа на основе полученной ранее таблицы базового секретного ключа. Затем датчик 53 случайных чисел временно отключается, и реализуется описанный выше алгоритм перестановки столбцов и строк таблицы базового секретного ключа. При этом полученная таблица внутреннего секретного ключа записывается в блок памяти 52 внутреннего ключа. Таким образом формируются таблицы базового, внешнего и внутреннего секретных ключей, необходимые для реализации защищенной передачи и обработки информации в сервере 3 распределенной обработки и пользовательском устройстве 2.

Подсистема 8 формирования открытых ключей (фиг.7)

Назначение этой подсистемы состоит в формировании открытых ключей для пользовательского устройства 2 (пользователь A) и сервера 3 распределенной обработки (пользователь B), обеспечивающих перевод их внешних секретных ключей в симметричное состояние. Как было отмечено выше, эта функция выполняется каждый раз при организации закрытой связи между пользователями A и B. При этом формирование открытых ключей производится с применением логического вывода на функционально связанных таблицах секретных перестановок столбцов и строк с использованием транзитивных зависимостей. Перед началом этого процесса в центре 1 сертификации, формирования и распределения ключей с использованием датчика 43 случайных чисел и схемы выбора 44 комбинаций подсистемы 5 формирования таблиц секретных ключей производится генерация последовательностей секретных перестановок столбцов и строк для симметричного внешнего ключа. Эти последовательности позволяют сформировать на основе таблицы главного секретного ключа, путем соответствующих перестановок столбцов и строк, симметричные таблицы внешнего секретного ключа для пользователей A и B. Однако учитывая, что сформированные таблицы начального, базового и внешнего секретных ключей каждого пользователя различны, необходимо провести логическую обработку соответствующих перестановок. При этом вычисляются относительные несекретные перестановки (открытые ключи) для пользователей A и B, позволяющие перевести их асимметричные таблицы внешних секретных ключей в симметричное (идентичное) состояние. С этой целью полученная в подсистеме 5 формирования закрытых ключей указанная секретная перестановка таблиц столбцов и строк записывается через информационно-логическую защищенную вычислительную систему 6, блок коммутации 67, блок 69 управления в блок памяти 62 для таблицы симметричной перестановки столбцов и строк таблиц внешних ключей.

В общем случае каждая последовательность секретной перестановки имеет следующий вид:

$1 \rightarrow i,\ 2 \rightarrow j,\ 3 \rightarrow l,\ ...,\ m \rightarrow k,\ ...,\ n \rightarrow r,$

где 1, 2, 3... n - порядковые номера исходных столбцов (строк) главного секретного ключа, i, j, l... r - их случайные номера перестановки. При этом порядковые номера образуют входной столбец таблицы перестановок, а случайные номера перестановок - выходной ее столбец.

После этого из подсистемы 5 формирования закрытых ключей в блок памяти 61 для таблиц секретных перестановок столбцов и строк секретных ключей переписываются все таблицы секретных перестановок для пользователя A (B). Эти таблицы, как было отмечено выше, позволяют на основе таблицы главного секретного ключа с использованием соответствующих перестановок столбцов и строк сформировать сначала таблицу начального секретного ключа, затем таблицы базового и внешнего секретного ключей. Указанные таблицы имеют функциональные зависимости между различными строками, которые можно определить путем выделения идентичных номеров в выходном столбце

каждой предыдущей таблицы и во входном столбце каждой последующей таблицы. При этом таблицы секретных перестановок располагаются в следующем порядке: таблицы для формирования начального секретного ключа, таблицы для формирования базового секретного ключа, таблицы для формирования внешнего секретного ключа (фиг.13). После этого в таблице секретных перестановок для формирования начального секретного ключа выделяется первая строка, и на основе функциональных связей формируется следующая транзитивная зависимость: $1 \rightarrow i, \rightarrow j, \rightarrow k$, которая связывает перестановки первого элемента главного секретного ключа на множестве указанных таблиц перестановок. Данная транзитивная зависимость записывается в регистр 63 последовательности транзитивной зависимости через блок коммутации 68 и блок 69 управления, а затем поступает в блок 64 логического вывода на последовательности транзитивной зависимости. Туда же поступает значение первой строки таблицы перестановки ($1 \rightarrow i$) из блока памяти 62 для таблицы симметричной перестановки столбцов и строк таблицы внешнего секретного ключа. В результате логического вывода исходная транзитивная последовательность дополняется соотношением $k \rightarrow i$ и принимает вид $1 \rightarrow i, \rightarrow j, \rightarrow k \rightarrow i=1 \rightarrow i$. Полученный результат логического вывода совпадает с первой строкой таблицы симметричной перестановки столбцов (строк) таблицы внешнего секретного ключа. При этом формируется первая строка относительной (несекретной) перестановки открытого ключа в виде $k \rightarrow i$. Затем такие же процедуры производятся со второй строкой таблицы секретной перестановки столбцов и строк начального секретного ключа, базового секретного ключа, таблицы симметричного внешнего ключа и т.д. В результате выполнения n процедур логического вывода будет сформирован открытый ключ в виде таблицы относительной перестановки столбцов (строк) для пользователя А (В). Отметим, что каждый открытый ключ содержит две таблицы перестановок (таблицу для столбцов и таблицу для строк). При этом для каждого пользователя формируется свой индивидуальный открытый ключ. Полученные относительные перестановки записываются в блок памяти 65 для таблицы относительной перестановки столбцов и строк таблицы внешнего ключа, а оттуда считываются в регистр 66 открытого ключа. Затем по команде блока 69 управления открытый ключ через блок коммутации 68 поступает в информационно-логическую защищенную вычислительную систему 6. Оттуда он передается через подсистему 11 распределения ключей по компьютерной системе пользователю А (В). После получения открытого ключа в пользовательском устройстве 2 или сервере 3 распределенной обработки он поступает в подсистему 13, 25 формирования таблиц секретных ключей. При этом открытый ключ, содержащий две таблицы перестановок, через блок коммутации 59 записывается в регистр 55 перестановки столбцов для формирования таблицы внешнего ключа и в регистр 56 перестановки строк для формирования таблицы внешнего ключа. Затем на основе таблицы асимметричного внешнего секретного ключа, записанного в блок памяти 51 таблицы внешнего ключа, путем соответствующей перестановки столбцов и строк производится формирование таблицы симметричного внешнего секретного ключа в пользовательском устройстве 2 и сервере 3 распределенной обработки.

Подсистема аутентификации и контроля целостности информации (фиг.8)

При передаче по системе связи открытых ключей между центром 1 сертификации, формирования и распределения ключей, пользовательским устройством 2 и сервером 3 распределенной обработки данных используется электронная цифровая подпись. Она основана на применении хэш-функции и личного секретного ключа пользователя.

Для реализации хэш-функции используют однонаправленную функцию, базирующуюся на применении технологии стохастического кодирования. Сначала рассмотрим порядок образования хэш-функции в режиме открытой передачи информации. Для рационального применения ресурсов при синтезе хэш-функции сообщения (документа), передаваемого пользователем А пользователю В, максимально задействуют алгоритмы организации закрытого режима. Поэтому с целью рационализации получения хэш-функции применяются процедуры формирования открытых ключей, перевод таблиц внешних секретных ключей в симметричный режим и сложение информации с использованием закрытого

арифметического процессора. Хэш-функция может использоваться не только для аутентификации электронных документов, но и для аутентификации пользователя при вводе его пароля в компьютер. С целью реализации хэш-функции для аутентификации передаваемых электронных документов в открытом режиме пользователи A и B запрашивают в центре сертификации открытые ключи-перестановки для приведения таблиц внешнего секретного ключа в симметричное состояние. При этом реализуется описанный выше алгоритм формирования и передачи открытого ключа для пользователей A и B. Полученный открытый ключ поступает в подсистему 13, 25 формирования таблиц секретных ключей пользовательского устройства 2 (пользователь A) и сервера 3 распределенной обработки (пользователь B). Далее используется описанный выше алгоритм перевода таблиц внешних секретных ключей пользователей A и B в симметричный режим. Полученная таблица из подсистемы 13, 25 формирования таблиц секретных ключей через блок управления 21, 30 защищенной обработкой поступает в блок 77 управления и внешний стохастический кодер 74 подсистемы 18, 33 аутентификации и проверки целостности информации. При этом происходит настройка внешнего кодера пользователей A и B на симметричный режим передачи. Затем начинается передача информации между пользователями A и B в открытом режиме. Одновременно с этим каждый передаваемый i-ый элемент данных (i=1-N) поступает во внешний стохастический кодер 74 подсистемы 18 аутентификации и проверки целостности информации и подвергается стохастическому кодированию и гаммированию. Затем полученный кодовый блок перекодируется в блоке памяти 75 столбцов перекодирования символов кодового блока в числовой код и поступает в блок управления 21 защищенной обработкой. После этого он подается в информационно-логическую защищенную вычислительную систему 20 и складывается в защищенном арифметическом процессоре 19 с предыдущим (i-1)-ым кодовым блоком и с i-ым кодовым блоком в стохастически преобразованном виде. В результате после передачи всех N элементов данных сообщения в защищенном арифметическом процессоре будет образована 64 байтная комбинация, являющаяся сжатым представлением переданного документа. В сервере 3 распределенной обработки (пользователь B) при приеме каждого i-го кодового блока сообщения выполняются те же процедуры формирования хэш-функции. После приема всех N кодовых блоков полученные по системе и сформированные в сервере 3 распределенной обработки значения хэш-функции поступают в блок управления 30 защищенной обработкой, а затем в подсистему 33 аутентификации и проверки целостности информации. В этой подсистеме по команде блока 77 управления указанные комбинации поступают в схему сравнения 76 значений хэш-функции. Здесь производится сравнение значения хэш-функции, переданной пользователем A, и хэш-функции, сформированной пользователем B. При совпадении указанных значений документа он считается аутентифицированным. За счет стохастического кодирования обеспечиваются следующие свойства:

- гарантированная защита с заданной вероятностью от любых изменений в тексте при его передаче (вставки, выбросы, перестановки и др.);
- уникальность полученной хэш-функции (вероятность того, что значения хэш-функций разных документов совпадут, ничтожно мала);
- необратимость хэш-функции, поскольку задача подбора документа, который обладал бы тем же значением хэш-функции, является вычислительно неразрешимой.

Такой же алгоритм формирования хэш-функции передаваемых сообщений применяется и в закрытом режиме. При этом у пользователя A формирование хэш-функции производится одновременно с кодированием передаваемых элементов данных, а у пользователя B реализация хэш-функции выполняется после декодирования каждого очередного блока с использованием процедуры повторного кодирования.

При формировании значения хэш-функции пароля во внешний стохастический кодер подсистемы 18, 33 аутентификации и проверки целостности информации записывается таблица базового ключа. Она обеспечивает заполнение таблиц указанного кодера. В этом случае кодированию подвергаются введенные из подсистемы 17 ввода информации с

носителя данных пароль и значение PIN-кода пользователя, которые записываются в регистры 70, 71 пароля и PIN-кода подсистемы 18, 33 аутентификации и проверки целостности информации. После сложения стохастически преобразованных комбинаций в защищенном арифметическом процессоре 19, 34 полученная комбинация длиной n поступает в информационно-логическую защищенную вычислительную систему 20, 35, где делится на отрезки заданной длины m<n, которые суммируются по mod 2. Затем полученное значение через блок управления 21, 30 защищенной обработкой поступает в схему сравнения значения хэш-функции и сравнивается со значением хэш-функции пароля, записанного на носитель данных сертифицированного пользователя (смарт-карту).При формировании электронной цифровой подписи пользователь А с помощью датчика случайных чисел подсистемы 5 формирования таблиц секретных ключей генерирует личный секретный ключ в виде перестановки строк таблицы внешнего секретного ключа. При этом с учетом данной комбинации перестраивается внешний стохастический кодер 74 подсистемы 18 аутентификации и проверки целостности информации. Затем в блоке управления 21 защищенной обработкой пользователя А вычисляется открытый ключ в виде относительной несекретной перестановки между предыдущим и новым расположением строк таблицы внешнего секретного ключа. Этот открытый ключ передается пользователю В и может быть передан в центр 1 сертификации с целью регистрации личного ключа пользователя А. На основе полученного открытого ключа пользователь В перестраивает таблицу внешнего секретного ключа для декодирования и проверки электронной подписи пользователя А. При формировании этого ключа используются функциональные зависимости между секретными перестановками соответствующих таблиц пользователей А и В. Открытый ключ для пользователя В может вычисляться также и в центре 1 сертификации, формирования и распределения ключей при регистрации личного ключа пользователя А. Для этого применяется сформированная пользователем А относительная несекретная перестановка и функциональные зависимости между секретными перестановками соответствующих таблиц пользователей А и В.

С помощью полученного сертифицированного ключа во внешнем стохастическом кодере 74 подсистемы 18 аутентификации и проверки целостности информации пользователя А производится преобразование сформированной при передаче документа комбинации его хэш-функции. Пользователь В при получении в конце сообщения кодированной хэш-функции осуществляет ее декодирование с использованием полученного открытого ключа и сравнение со сформированным ранее значением хэш-функции принятого сообщения.

Стохастический кодер (фиг.9)

Рассмотрим более подробно процесс синтеза и функционирования стохастического кодера (15, 74) пользовательского устройства 2 и сервера 3 распределенной обработки, а также декодера 14 на основе полученных таблиц внутреннего или внешнего секретных ключей. Отметим, что функции кодера (декодера), описанные ниже, могут выполнять также устройства стохастического перекодирования (23, 24 на фиг.3, 27, 28, 29 на фиг.4), входящие в состав пользовательского устройства 2 и сервера 3 распределенной обработки. Поэтому описание процесса функционирования стохастического кодера (декодера) 15 (14) является общим для целого ряда указанных устройств.

Работа стохастического кодера основана на использовании таблиц внутреннего (внешнего) секретного ключа. Для этого таблица внутреннего (внешнего) секретного ключа делится на две части размером (m * m/2). Первая часть таблицы используется для заполнения блока регистров 79-1, 79-2,...,79-n столбцов многоалфавитного кодера (фиг.9), вторая применяется в схеме 84 формирования гаммы (n=m/2). Содержимое регистров циклической перестановки 81, 90 формируется на основе таблицы перестановки строк соответствующей таблицы базового или внешнего ключа. В процессе обмена информации их содержимое периодически изменяется под воздействием датчика 53 случайных чисел подсистемы 13 формирования таблиц секретных ключей пользовательского устройства 2 передающей стороны. При этом на приемную сторону

посылается полученная в блоке управления 21 защищенной обработкой относительная перестановка между предыдущими (не более n) и последующим состоянием циклических регистров перестановки 81, 90. Эта комбинация вычисляется в блоке управления 21 защищенной обработкой с использованием алгоритма формирования открытого ключа, основанного на применении логического вывода на транзитивных зависимостях таблиц перестановок. Данный алгоритм является аналогом алгоритма формирования открытых ключей, реализованного в подсистеме 8 формирования открытых ключей. Полученная при этом относительная перестановка является открытым ключом, которым периодически обмениваются пользователи A и B в ходе закрытой передачи данных. При этом пользователь B, получив от пользователя A второй открытый ключ, в блоке управления 30 защищенной обработкой своевременно вычисляет новую комбинацию для записи в циклический регистр перестановки 81, 90. Вычисление этой комбинации производится на основе значения предыдущей комбинации циклических регистров перестановки 81, 90 и полученного открытого ключа. Поэтому стохастические кодеры 15 и декодеры 14 каждого пользователя будут иметь идентичные случайные комбинации в циклических регистрах перестановки 81, 90. Кроме этого в процессе обмена закрытой информацией между пользователями A и B сформированные случайные комбинации, переданные с помощью открытых ключей, могут периодически применяться для синхронной замены содержимого входного (выходного) регистра 78 перестановки стохастического кодера (декодера) 15, 14. Полученные случайные комбинации могут использоваться также в пользовательском устройстве 2 и сервере 3 распределенной обработкой для поэтапной замены содержимого столбцов блока регистров 79-1, 79-2,...,79-n столбцов многоалфавитного кодера и блока регистров 88-1, 88-2,....88-n таблицы формирования гаммы (фиг.9).

В общем случае в блоке управления защищенной обработкой 21, 30 на основе очередного открытого ключа и таблиц секретных ключей могут быть сформированы от 1 до m новых случайных последовательностей. Эти последовательности применяются для замены требуемого числа комбинаций регистров столбцов блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера и комбинаций регистров столбцов блока регистров столбцов 88-1, 88-2,...,88-n таблицы формирования гаммы.

Описанные процедуры периодической замены содержимого циклических регистров перестановки 81, 90, входных (выходных) регистров 78 и столбцов блока регистров 79-1, 79-2,...,79-n столбцов многоалфавитного кодера и блока регистров 88-1, 88-2,...,88-n таблицы формирования гаммы обеспечивают фактическую модификацию таблиц внутреннего (внешнего) ключей путем случайной перестановки столбцов, строк и их поэтапной замены. Такие же процедуры выполняются в устройствах стохастического перекодирования 23, 24, 25, 27, 29 пользовательского устройства 2 и сервера 3 распределенной обработки при выполнении ими функций кодеров (декодеров). Эти функции направлены на повышение вычислительной стойкости системы. При этом от выбора периодичности указанных функций перестановки и замены зависит гарантированный уровень защищенности процессов передачи и обработки информации. В нормальном режиме функционирования описанные процедуры модификации таблиц внешних (внутренних) ключей с использованием открытых ключей выполняются после передачи N и более кодовых блоков. В режиме повышения уровня защищенности период модификации таблиц внешних (внутренних) ключей стохастических кодеров (декодеров) с помощью открытых ключей может сокращаться вплоть до перехода к режиму применения одноразовых таблиц внешних (внутренних) ключей. Этот режим, имеющий максимальный уровень защищенности, будет описан ниже.

Таким образом, периодическая модификация таблиц внешних (внутренних) секретных ключей с помощью открытых ключей является описанной выше системной функцией, направленной на обеспечение заданного уровня защищенности процесса передачи информации.

Для обеспечения защиты процесса обмена информации по шинам компьютера используются внутренние стохастические кодеры 15. При этом блок регистров 79-1, 79-

2,...,79-n столбцов многоалфавитного кодера заполняется на основе случайной информации, содержащейся в первой части таблицы внутреннего секретного ключа. Для схемы 84 формирования гаммы применяется вторая часть указанной таблицы.

Рассмотрим пример построения и функционирования стохастического кодера 15 с конкретными параметрами: m=256 байт, длина кодового блока N=64 байта, число столбцов n=m/2=128 байт. Он имеет циклический регистр 31 перестановки длиной m/2=128 байт, схему 80 подключения столбцов, блок ключей-инверторов 82-1, 82-2,...,82-n и рекуррентный регистр 83, который описывается неприводимым многочленом вида $P(x^{127})=x^{127}+x+1$.

Для функционирования кодера в соответствии с перестановкой строк таблицы внешнего ключа производится перестановка входной ASCII таблицы алфавитно-цифрового кода, содержащей 256 строк. Эта таблица записывается во входной регистр 78 перестановки.

При формировании входной таблицы перестановки в нее кроме ASCII кода (строки 1-127) вводят строки для двухбайтных числовых комбинаций (00-99), а также для специальных управляющих символов (текстовый блок, числовой блок, открытый блок, закрытый блок, числовой блок целочисленный, с фиксированной запятой, плавающей запятой и др.).

При реализации обмена в закрытом режиме информация, набираемая на клавиатуре, кодируется с помощью внутреннего стохастического кодера 15 и преобразуется в защищенные 64 байтные блоки. В этом случае для каждого блока информации формируется своя кодовая таблица, содержащая 64 столбца и 256 строк. Выбор столбцов блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера происходит с помощью рекуррентного регистра 83 и циклического регистра 81 перестановки, куда записана очередная случайная комбинация перестановки длиной n байт. В рекуррентном регистре 83 путем выполнения последовательности очередных, начиная с 000...1, сдвигов, выбирается 127 байтная комбинация, которая содержит N>64 единиц. Позиция «1» в полученной комбинации рекуррентного регистра 83 с учетом случайной перестановки циклического регистра 81 определяет, какие из столбцов блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера используются для кодирования вводимого очередного элемента данных. При этом по сигналу блока 87 управления может производиться циклический сдвиг n-байтной случайной комбинации, записанной в каждый i-й столбец блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера, на случайное число байт, записанное в i-й ячейке циклического регистра 81 перестановки. После этого производится посимвольное кодирование методом замены в многоалфавитном кодере очередной информационной комбинации, поступающей из входного регистра 78 перестановки. При этом для кодирования каждого j-го символа, записанного в i-й строке входного регистра 78 перестановки, применяется случайный код в i-й строке соответствующего столбца, циклически сдвинутого на случайное число байт (от 0 до 256). Этот столбец входит в состав 64 столбцов, выбранных с учетом комбинации рекуррентного регистра 83 и циклического регистра 81 перестановки. Для кодирования следующего блока вновь выполняются последовательные сдвиги рекуррентного регистра 83 до получения новой комбинации, содержащей n>64 единиц. При этом производится циклический сдвиг на один байт случайной комбинации, записанной в циклический регистр 81 перестановки. После этого в соответствии с новой комбинацией в регистре 81 производится случайный циклический сдвиг комбинации, записанной в каждый i-й столбец блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера.

Поскольку многочлен $P(x^{127})$ является неприводимым, то соответствующий ему рекуррентный регистр обеспечивает последовательную генерацию всех $(2^{127}-1)$ возможных различных комбинаций. Следовательно, для кодирования каждого очередного блока применяется новый многоалфавитный код (одноразовый ключ), определяемый очередной комбинацией рекуррентного регистра 83, которая включает N>64 единиц, а также содержимым циклического регистра 81 перестановки и случайной комбинацией входного регистра 87 перестановки.

Если очередная комбинация рекуррентного регистра 83 содержит число единиц N<64, то по сигналу блока 87 управления происходит инверсия данной комбинации в блоке ключей-инверторов 82-1, 82-2,...,82-n. Тогда она будет включать N>64 единиц. После передачи N кодовых блоков по сигналу блока управления 21 защищенной обработкой реализуется описанная выше системная функция модификации таблицы внутреннего (внешнего) ключей стохастических кодеров (декодеров) с использованием открытого ключа. При этом по команде блока 87 управления происходит циклический сдвиг комбинаций, записанных в регистры блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера, для возвращения их в исходное состояние.

Каждый кодируемый элемент данных может содержать либо слово (элемент текста), либо число с указанием формы представления (целочисленное, с фиксированной или плавающей запятой).

При вводе текстовой информации каждый i-й символ кодируется после первоначальной перестановки (в соответствии с таблицей внешнего ключа) с использованием i-го столбца блока регистров 79-1, 79-2,...,79-n столбцов многоалфавитного кодера. При этом номер строки j данного столбца определяется согласно номеру j строки, соответствующей данному символу в таблице начальной перестановки.

После ввода текстового элемента автоматически формируется служебная четырехбайтная комбинация, содержащая указанные выше служебные символы. Эта комбинация одновременно выполняет функцию имитозащиты.

Если длина текстовой комбинации меньше 60, то оставшиеся позиции заполняются кодированными числовыми значениями. Они формируются путем многоалфавитного кодирования числовой комбинации с номером i, которая является первой после j-го символа, завершающего текстовый элемент данных, если двигаться по таблице входной перестановки.

При вводе числового элемента данных во входном регистре 78 перестановки производится формирование числовых комбинаций вправо и влево от запятой по (m=2) цифр. Затем осуществляется их кодирование путем обращения ко входной таблице (строки 128-256) и преобразования с помощью блока регистров 79-1, 79-2,...,79-n столбцов многоалфавитного кодера. При этом каждая очередная комбинация j в составе числа превращается в стохастический индекс $I_{\xi_j}^{(u)}$ посредством кодирования с использованием j-го столбца. После числовой комбинации, длина которой должна быть не более 60 байт, в состав формируемого кодового блока следует служебная комбинация. Если число меньше, чем 60 байт, то после завершения числа включается служебная комбинация (4 байта). Затем вводится переменный код буквы с номером i, которая следует по входной таблице перестановок сразу же после j-й, завершающей m-байтной числовой комбинации.

Полученные кодовые блоки поступают в сумматор по mod 2 85 для сложения с гаммой, выданной из схемы 84 формирования гаммы, и затем записываются в выходной регистр 86 кодового блока.

Схема формирования гаммы (фиг.10)

При синтезе схемы 84 формирования гаммы используется вторая часть таблицы внутреннего (внешнего) кода размером (m*m/2). Она применяется для заполнения блока регистров столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n (фиг.10). Для рассмотренного выше примера схема формирования гаммы (фиг.10) содержит таблицу с параметрами m=256 байт, n=m/2=128 байт, аналогичный рекуррентный регистр 92, блок ключей-инверторов 91-1, 92-2,...,92-n, циклический регистр 90 перестановки длиной m= 128 байт, а также схему 89 подключения столбцов, сумматор по mod 2 94 длиной 256 байт и регистр исходной гаммы длиной 64 байта.

Как было отмечено выше, после формирования очередного кодового блока производится его гаммирование путем сложения с 64 байтной гаммой в сумматоре по mod 2 85. Эта случайная последовательность генерируется в схеме 84 формирования гаммы. При этом сначала под управлением комбинации, полученной в рекуррентном регистре 92

после очередного i-го сдвига исходной комбинации 000...01 с использованием циклического регистра 90 перестановки и схемы 89 подключения столбцов, производится выборка соответствующих столбцов из блока регистров столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n. Выбираются те из 128 столбцов, номерам которых в i-й последовательности соответствует «1». По сигналу блока 96 управления схемы формирования гаммы может быть реализована процедура циклического сдвига каждой случайной комбинации, записанной в блок регистров столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n, на случайное число байт. Эта процедура выполняется также, как и в стохастическом кодере 15. При этом используется комбинация случайной перестановки, записанная в регистр 90 циклической перестановки после реализации очередного цикла модификации таблицы внутреннего (внешнего) ключа стохастического кодера. Число единиц в выбранной последовательности должно быть не менее заданного значения t ($2<t<N$). Это обеспечивает блок управления 95 схемы формирования гаммы. Затем выбранные столбцы, каждый из которых представляет собой случайную 256-байтную комбинацию, через ключ 95 поступают в сумматор по mod 2 94, где выполняется их сложение по mod 2. Полученную в результате случайную комбинацию записывают в регистр 93 исходной гаммы и затем пересылают в блок 96 управления схемы формирования гаммы. Здесь выполняется очередное преобразование исходной гаммы. Для этого может использоваться функция перестановки с применением очередной случайной комбинации длиной m. Эта комбинация, полученная из блока 87 управления, используется для очередной модификации таблицы внешнего (внутреннего) секретного ключа стохастического кодера 15. При этом данная комбинация применяется для замены содержимого заданного числа столбцов блока регистров столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n, а также для замены содержимого циклического регистра 90.

Второй вариант преобразования комбинации исходной гаммы заключается в использовании процедуры ее шифрования с применением программной реализации стандарта шифрования DES (AES). При этом в качестве ключа для данного алгоритма шифрования используется отрезок очередной случайной комбинации, применяемой для модификации таблиц внешнего (внутреннего) секретного ключа. Полученную в результате преобразования исходной гаммы комбинацию делят на четыре отрезка по 64 байта и суммируют по mod 2. В результате будет получена случайная комбинация, записываемая в регистр 93 исходной гаммы. Эта комбинация может непосредственно применяться для гаммирования очередного кодового блока или использоваться с целью формирования N различных случайных последовательностей, предназначенных для гаммирования N очередных кодовых блоков (N=64). В первом случае сформированная комбинация из регистра 93 исходной гаммы через блок управления 96 схемы формирования гаммы и ключ 95 поступает в сумматор по mod 2 82 стохастического кодера 15.

Отметим, что схема формирования гаммы обеспечивает первоначально генерацию (2^{127}-1) различных значений случайных комбинаций. Своевременная замена содержимого таблицы формирования гаммы позволяет сделать период данного ДСЧ бесконечным. При этом изменение содержимого блока регистров столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n производится при смене в компьютерах системы защиты таблиц начальных ключей. Этот процесс осуществляется регулярно центром 1 сертификации, формирования и распределения ключей с использованием открытых ключей-перестановок. Кроме этого, как было показано выше, частичная замена содержимого столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n производится в процессе обмена информации между пользователями A и B с использованием открытых ключей при реализации системной функции модификации таблицы внешнего (внутреннего) ключа. При этом происходит также замена содержимого циклического регистра 90 перестановки.

Во втором случае формирование N последовательностей гаммы для кодовых блоков производится путем кодирования полученной исходной гаммы методом "распыления и замены". Для этого применяется блок регистров столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n, который имеет n=128 столбцов длиной по 256 байт. Он используется

для получения каждого из N=64 блоков гаммы. В отличие от формирования кодовых блоков, которое производится построчно с применением всех N столбцов, генерация N=64 блоков гаммы осуществляется путем кодирования исходной гаммы по столбцам. При этом для формирования j-й гаммы применяются столбцы с номером j и (j+1), образуя "таблицу распыления и замены". С целью получения гаммы для очередного блока j (j=1, N) исходная гамма обращается к j-му столбцу, находит в нем идентичную комбинацию Uji для каждого байта Uji гаммы Uj. Затем происходит замена кода Uji на код Uj+1,i (Uji $\rightarrow$ Uj+1,i).

Кодирование и замена 64 байтной исходной гаммы производится по всей длине столбцов, равной 256 байт («распыление» 64 байта по 256 байт с последующей их заменой на коды следующего столбца). Каждая полученная гамма с номером j=(1-64) складывается в сумматор по mod 2 82 стохастического кодера 15 с очередным j-м блоком, поступающим из блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера.

Таким образом, стохастический кодер 15 с использованием схемы 84 формирования гаммы обеспечивает стохастическое кодирование и гаммирование последовательности передаваемых блоков в режиме одноразового ключа. В начале сформированной последовательности передаются переменные значения многочленов и начальных комбинаций рекуррентных регистров 83, 92 длиной 16 байтов каждый. Отметим, что переменные значения многочленов рекуррентных регистров 83, 92 формируются в блоке управления защищенной обработкой 21, 30.

Эти комбинации включаются в служебный блок, который передается в начале последовательности из N информационных блоков в закрытом виде. Для шифрования служебного блока применяется секретная перестановка, сформированная в блоке управления защищенной обработкой (21, 30). Она вычисляется на основе комбинации открытого ключа, используемой для очередной модификации таблиц секретного внешнего (внутреннего) ключа стохастического кодера 15.

Служебный блок после дешифрования применяется для настройки регистров стохастического декодера 14, который имеет идентичную таблицу внешнего (внутреннего) ключа и, соответственно, обеспечивает корректное декодирование всех N блоков, поступающих во входной регистр кодового блока. При этом в таблицу выходного регистра перестановки записывается обратная таблица входной перестановки, используемой в стохастическом кодере 15.Описанные функции формирования, шифрования и дешифрования служебного блока применяются также при использовании устройств стохастического перекодирования 23, 24, 27, 28 и 29 для передачи и обработки информации. Эти функции реализуются в блоках управления защищенной обработкой 21, 30 пользовательского устройства 2 и сервера 3 распределенной обработки с использованием соответствующих открытых ключей.

Отметим, что режим одноразового ключа в стохастическом кодере 15 может быть реализован без применения функции гаммирования. В этом случае процесс преобразования информации в стохастическом кодере 15 (стохастическом декодере 14) производится с отключением по сигналу блока 87 управления схемы 84 формирования гаммы (фиг.9). При этом символы кодового блока, сформированные в блоке регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера, поступают без изменения через сумматор по mod 2 85 в выходной регистр 86 кодового блока.

Описанная схема формирования гаммы используется также в устройствах стохастического перекодирования 23, 24 пользовательского устройства 2 и в устройствах стохастического перекодирования 25, 27, 29 сервера 3 распределенной обработки.

Таким образом, для защиты информации, передаваемой по компьютерной сети между пользовательским устройством 2 (пользователь A) и сервером 3 распределенной обработки (пользователь B), а также при внутрикомпьютерном обмене реализуется режим "одноразового ключа", в соответствии с которым каждый кодовый блок передаваемой последовательности кодируется своим ключом. Каждый ключ является уникальным на множестве передаваемых блоков. При этом для обеспечения заданного уровня защищенности при передаче информации в указанных выше стохастических кодерах

(декодерах) 14, 15 и устройствах стохастического перекодирования (23, 24, 25, 27, 29) реализуется описанная выше системная функция модификации таблицы внешнего (внутреннего) ключа.

В процессе реализации этой функции при передаче информации возможно сокращение периода модификации ключевых таблиц вплоть до перехода к режиму применения одноразовых таблиц внешних (внутренних) ключей. Этот режим, имеющий максимальный уровень защищенности, предполагает передачу нового открытого ключа после каждого очередного кодового блока. По этому ключу в стохастическом кодере (декодере) в соответствии с описанным выше алгоритмом производится запись новой случайной комбинации в циклические регистры перестановки 81, 90, во входной (выходной) регистр перестановки 78 и замена случайной комбинации одного из столбцов блока регистров столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n. Именно эта случайная комбинация по сигналу блока 95 управления вместе с другими t, случайно выбранными комбинациями блока регистров столбцов таблицы формирования гаммы 88-1, 88-2,...,88-n применяется при формировании гаммы для очередного кодового блока. Таким образом, в этом режиме, также как и в классической схеме одноразового ключа, для шифрования каждого очередного блока длиной N применяется одноразовая случайная комбинация длиной N. При этом для кодирования каждого очередного блока применяется одноразовый сформированный случайным образом многоалфавитный кодер. Устройство стохастического перекодирования (фиг.11А, 11Б)

Важное значение для создания единого защищенного контура передачи и обработки данных имеют устройства стохастического перекодирования (23, 24 на фиг.3, 27, 28, 29 на фиг.4), входящие в состав пользовательского устройства 2 и сервера 3 распределенной обработки. Они реализуют дополнительное шифрование защищенной информации для ее адаптации к передаче в среде компьютера или по компьютерной системе, а также к различным видам обработки путем стохастического преобразования без раскрытия содержания данных.

Эти устройства имеют единую структуру (фиг.11А, 11Б), но, исходя из функционального назначения, делятся на три типа: «внутренний код - внешний код», «внешний код - внутренний код» и «внутренний код 1 - внутренний код 2». Основу указанных устройств составляют элементы первой и второй ступеней стохастического преобразования 98, 101, у которых идентичная структура, практически совпадающая со структурой стохастического кодера 15. Отметим, что первая ступень 98 стохастического преобразования при необходимости может выполнять функции стохастического декодера, а вторая ступень 101 стохастического преобразования может использоваться в режиме стохастического кодера.

Устройство стохастического перекодирования типа «внутренний код - внешний код» обеспечивает возможность передачи информации, закодированной с помощью внутреннего кода, по компьютерной системе после установления засекреченной связи между пользовательским устройством 2 и сервером 3 распределенной обработки данных. Перекодирование передаваемой информации происходит без раскрытия ее содержания. Для выполнения этой функции первая ступень 98 стохастического преобразования по служебной комбинации, содержащей многочлен и значение рекуррентного регистра, и открытому ключу настраивается на обработку первого из числа N кодовых блоков, поступающих по шинам компьютера от внутреннего кодера. При этом блок регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера и блок регистров столбцов 88-1, 88-2,...,88-n таблицы формирования гаммы первой ступени 98 стохастического преобразования заполняются на основе таблицы внутреннего ключа аналогично внутреннему стохастическому кодеру 15. В циклический регистр 81 перестановки, в регистр перестановки 99 и схему 84 формирования гаммы записывается случайная комбинация, вычисленная описанным выше образом в блоке управления 30 защищенной обработкой. Вторая ступень 101 стохастического преобразования настраивается с помощью таблицы внешнего ключа как внешний стохастический кодер 74 для обеспечения симметричной закрытой связи с сервером 3 распределенной обработки. Для подключения и

согласования первой ступени 98 стохастического преобразования со второй ступенью 101 стохастического преобразования блок управления 21 защищенной обработкой пользовательского устройства 2 формирует относительные перестановки, которые через блок 87 управления записывает в регистр перестановки 100. Вторая ступень 101 стохастического преобразования, выполняя функции кодера, описанным выше порядком вводится в симметричный режим закрытой передачи с первой ступенью 98 стохастического преобразования устройства 25 стохастического перекодирования сервера 3 распределенной обработки. При этом обеспечивается реализация системной функции модификации таблицы внешнего ключа с помощью периодически передаваемого открытого ключа в устройствах стохастического перекодирования 24, 25.

Преобразование каждого очередного кодового блока из входного регистра, начиная с первого, производится посимвольно. Для этого в первой ступени 98 стохастического преобразования и во второй ступени 101 стохастического преобразования по сигналу блока 87 управления включаются регистры столбцов блоков регистров столбцов 79-1, 79-2,..., 79-n, использующиеся с целью кодирования первого символа кодового блока. Затем для каждого кодового блока в схеме 84 формирования гаммы генерируется соответствующая случайная последовательность и в ней выделяется первый символ, использующийся для гаммирования первого символа данного кодового блока. Этот символ суммируется по mod 2 с каждым символом регистра столбца блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера первой ступени 98 стохастического преобразования, который использовался для кодирования первого символа кодового блока во внутреннем стохастическом кодере 15. Такое же сложение выполняется с использованием первого символа гаммы и символов регистра столбца блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера второй ступени 101 стохастического преобразования, включенного для кодирования первого символа кодового блока внешнего кода. После этого в первой ступени 98 стохастического преобразования производится сравнение первого символа принятого кодового блока внутреннего кода с каждым из символов включенного регистра столбца блока регистров столбцов 79-1, 79-2,..., 79-n многоалфавитного кодера. При совпадении одного из сравниваемых значений с первым символом кодового блока этот символ считается идентифицированным (определена строка столбца регистра, которая имеет код, идентичный первому символу кодового блока). В этом случае блок 87 управления через ключ 108 и регистр перестановки 99, 100 обеспечивает передачу данного символа по соответствующей шине в регистр столбца первого символа внешнего кода блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера второй ступени 101 стохастического преобразования. В результате происходит замена первого символа кодового блока внутреннего кода (без снятия с него гаммы и декодирования) на первый гаммированный символ внешнего кода. Затем такая же процедура перекодирования производится с каждым очередным символом кодового блока внутреннего кода, пока не будет сформирован кодовый блок внешнего кода, содержащий в закрытом виде идентичную информацию. При этом, как следует из описания данной процедуры, перекодирование производится без раскрытия содержания защищенной информации. Перекодированный кодовый блок по сигналу блока 87 управления через ключ 108 записывается в выходной регистр 102 кодового блока второй ступени 101 стохастического преобразования. В результате происходит замена символов первого кодового блока. После этой замены блоки 87 управления производят необходимую смену комбинации в рекуррентных регистрах 83 и циклических регистрах 81 перестановки, подготавливая тем самым первую и вторую ступени стохастического преобразования 98, 101 для перекодирования следующего кодового блока. Затем осуществляется перекодирование очередного кодового блока и запись его в выходной регистр 102 кодового блока. После записи в выходной регистр 102 кодового блока всей последовательности N кодовых блоков внешнего кода в начало записывается служебный блок с начальной комбинацией, с многочленами рекуррентного регистра 83, 92 и производится передача защищенной последовательности кодовых блоков по

компьютерной системе в сервер 3 распределенной обработки.

Как было отмечено выше, в случае необходимости вторая ступень 101 стохастического преобразования может выполнять функции стохастического кодера. В этом случае блок 87 управления отключает первую ступень 98 стохастического преобразования, в регистр 100 перестановки второй ступени 101 стохастического преобразования записывается входная таблица перестановки и производится перевод всех элементов второй ступени 101 стохастического преобразования в режим функционирования стохастического кодера. Таким образом, на передаче пользовательского устройства 2 реализован первый тип устройства стохастического перекодирования: «внутренний код - внешний код».

На приеме в сервере 3 распределенной обработки применяется второй тип устройства стохастического перекодирования: «внешний код - внутренний код». Это устройство 28 стохастического перекодирования описанным выше порядком обеспечивает преобразование кодовых блоков внешнего кода в кодовые блоки внутреннего кода без раскрытия содержания информации. Для выполнения этой функции первая ступень 98 стохастического преобразования по служебной комбинации, содержащей многочлен и значение рекуррентных регистров 83, 90, настраивается на обработку первого из числа N кодовых блоков, которые поступают в приемо-передающий блок 31 сервера 3 распределенной обработки. При этом блок регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера и блок регистров столбцов 88-1, 88-2,...,88-n таблицы формирования гаммы первой ступени 98 стохастического преобразования заполняются на основе таблицы внешнего ключа. Вторая ступень 101 стохастического преобразования настраивается с помощью таблицы внутреннего ключа как внутренний стохастический кодер 15 для обеспечения симметричной закрытой передачи информации в среде сервера 3 распределенной обработки. Для подключения и согласования первой ступени 98 стохастического преобразования со второй ступенью 101 стохастического преобразования блок управления 21 защищенной обработкой пользовательского устройства 2 формирует соответствующие относительные перестановки, которые через блок 87 управления записывает в регистры перестановки 99. После этого перекодирование каждого очередного принятого кодового блока, начиная с первого, производится посимвольно описанным выше порядком. Преобразованные кодовые блоки записываются через блок управления 30 защищенной обработкой в память информационно-логической защищенной вычислительной системы 35 сервера 3 распределенной обработки.

В процессе передачи сообщения пользователь А (пользовательское устройство 2) по случайным комбинациям, получаемым от датчика 53 случайных чисел, через схему 54 выбора комбинаций подсистемы 25 формирования таблиц секретных ключей (фиг.6) с использованием открытого ключа, вычисленного в блоке управления 21 защищенной обработкой, может производить описанную выше реализацию системной функции модификации таблиц внешних ключей. При этом обеспечивается периодическая замена содержимого циклического регистра 81, 90 перестановки, регистров перестановки 100, 99 устройств стохастического перекодирования 24, 25, а также замена заданного числа комбинаций блока регистров столбцов 79-1, 79-2,...,79-n и блока регистров таблицы формирования гаммы 88-1, 88-2,...,88-n схемы 84 формирования гаммы. Для формирования открытого ключа применяются представленным выше порядком предыдущие комбинации, которые были записаны в циклический регистр 81, 90 перестановки, и вновь полученная комбинация от датчика 53 случайных чисел. При этом используется алгоритм вычисления открытого ключа с логическим выводом на транзитивных зависимостях таблиц перестановок, реализованный в подсистеме 8 формирования открытых ключей (фиг.7). В блоке управления 30 защищенной обработкой пользователя В на основе полученного открытого ключа с использованием логического вывода и предыдущих таблиц циклического регистра 81 перестановки вычисляется новая секретная перестановка. После этого производится синхронный переход на новую случайную комбинацию циклического регистра 81, 90 перестановки, регистра перестановки 100, 99 в устройстве 24 стохастического перекодирования пользователя А и в устройстве

25 стохастического перекодирования пользователя B.

Подобным образом, как было показано выше, может осуществляться частичная замена столбцов таблиц внешнего ключа в устройстве 24 стохастического перекодирования пользователя A и в устройстве 28 стохастического перекодирования пользователя B (сервера 3 распределенной обработки). При этом обеспечивается синхронная замена содержимого регистров столбцов блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера и блока регистров столбцов 88-1, 88-2,...,88-n таблицы формирования гаммы, соответственно, второй ступени 101 стохастического преобразования пользовательского устройства 2 и первой ступени 98 стохастического преобразования сервера 3 распределенной обработки.

После посимвольного преобразования принятой последовательности N кодовых блоков в устройстве стохастического перекодирования сервера 3 распределенной обработки данных полученное сообщение, защищенное внутренним кодом, записывается через блок управления 30 защищенной обработкой в память информационно-логической защищенной вычислительной системы 35 сервера 3 распределенной обработки.

Таким образом, для защиты информации, передаваемой в среде компьютера, также, как и при внешнем закрытом обмене, реализуется концепция "одноразового ключа", в соответствии с которой каждый кодовый блок последовательности в устройстве стохастического перекодирования кодируется своим ключом. При этом данный ключ является уникальным на множестве N передаваемых блоков, а таблицы секретных ключей и перестановок периодически модифицируются с помощью открытых ключей в ходе реализации системной функции повышения уровня защищенности передаваемой информации.

После завершения сеанса закрытой связи между пользователями A и B симметричная таблица внешнего ключа (с разрешения центра 1 сертификации, формирования и распределения ключей) может использоваться как основа для формирования новой таблицы внешнего ключа при организации очередного сеанса закрытой симметричной связи. Для получения новой симметричной таблицы внешнего ключа производится перестановка столбцов и строк предыдущей таблицы внешнего ключа у пользователей A и B. При этом применяются описанный выше алгоритм вычисления открытых ключей в блоках управления 21, 30 защищенной обработкой и алгоритм модификации таблицы внешнего ключа в подсистеме 13, 25 формирования таблиц секретных ключей пользовательского устройства 2 и сервера 3 распределенной обработки.

Процесс шифрования защищенной таблицы 37 адресов электронной почты, защищенных таблиц 39 данных и защищенных Web-страниц 38 производится с использованием внутреннего устройства 29 стохастического перекодирования, которое относится к третьему типу «внутренний стохастический код 1 - внутренний стохастический код 2». Это устройство подключено к блоку управления 30 защищенной обработкой и защищенной информационно-логической вычислительной системе 35. При этом оно используется в режиме внутреннего стохастического кодера.

В процессе шифрования защищенной таблицы 37 адресов электронной почты в качестве последовательности N кодовых блоков рассматриваются элементы каждой строки таблицы. В результате после шифрования, которое обеспечивается блоком управления 30 защищенной обработкой и защищенной информационно-логической вычислительной системой 35, каждая строка содержит (N+1) полей. Первое поле является служебным, включает зашифрованные начальные комбинации и многочлены рекуррентных регистров 83, 92, которые использовались при кодировании данной строки. При этом формируется отдельная таблица открытых ключей - случайных комбинаций длиной n байт каждая. Указанные комбинации использовались для модификации таблицы внутреннего ключа при кодировании каждой из строк защищенной таблицы 37 адресов. Они также применялись для шифрования указанных выше комбинаций служебного поля. При этом номер каждой комбинации таблицы открытых ключей соответствует номеру строки защищенной таблицы 37 адресов, при кодировании которой она использовалась.

Такую же структуру имеют защищенные таблицы 39 данных.

При шифровании защищенных Web-страниц 38 каждая из них преобразуется во множество последовательностей из N кодовых блоков. В начале каждой последовательности N кодовых блоков записан соответствующий открытый ключ, который использовался для модификации таблицы внутреннего ключа при кодировании данной последовательности кодовых блоков. В начале зашифрованной Web-страницы записывается зашифрованный служебный блок с начальной комбинацией и многочленом рекуррентного регистра. Дешифрирование служебных блоков (служебных полей таблиц) производится с использованием соответствующих открытых ключей в блоке управления 30 защищенной обработкой перед реализацией заданных функций обработки защищенной информации.

Если в блоке управления 30 защищенной обработкой определено, что принятое зашифрованное сообщение является электронной почтой, то осуществляется обработка только закодированной адресной части сообщения. Цель обработки - определение адреса сервера 3 распределенной обработки, которому необходимо передать зашифрованное сообщение электронной почты. Для этого в защищенной таблице 37 адресов электронной почты необходимо найти соответствующую строку. Она должна содержать закодированный адрес пользовательского устройства 2 получателя и адрес сервера 3 распределенной обработки, которому требуется передать сообщение. Указанная процедура выполняется с помощью внутреннего устройства 29 стохастического перекодирования, подключенного к блоку управления 30 защищенной обработкой и защищенной информационно-логической вычислительной системе 35. В результате адрес получателя сообщения будет перекодирован без раскрытия его содержания в код, которым защищен адрес получателя первой строки таблицы. После этого полученный код и закодированный адрес первой строки таблицы считываются в защищенную информационно-логическую вычислительную систему 35 для сравнения. При совпадении сравниваемых значений из таблицы считывается поле, включающее код адреса сервера 3 защищенной обработкой, которому необходимо передать полученное зашифрованное сообщение. Затем закодированное сообщение электронной почты из защищенной информационно-логической вычислительной системы 35 поступает в блок управления 30 защищенной обработкой и далее в устройство стохастического перекодирования 28 приемопередающего блока 26 стохастического преобразования для передачи в закрытом виде выбранному серверу 3 распределенной обработки.

Если сравниваемые закодированные значения адресов не совпали, то внутреннее устройство 29 стохастического перекодирования переводит код адреса сообщения в код, которым закодирован адрес второй строки защищенной таблицы 37 электронной почты, для поиска нужного адреса в защищенном виде и т.д. Процесс поиска продолжается до тех пор, пока не будет найден требуемый адрес для отправки сообщения.

Если в блоке управления 30 защищенной обработкой по формату сообщения будет определено, что тип обработки полученной закодированной информации - арифметические вычисления, то зашифрованные операнды и коды арифметических вычислений поступают в защищенную информационно-логическую вычислительную систему 35. При этом по сигналу блока управления 30 защищенной обработкой первая ступень 98 стохастического преобразования устройства 29 стохастического перекодирования настраивается на внутренний код, которым защищено полученное сообщение. Одновременно с этим вторая ступень 101 стохастического преобразования во взаимодействии с защищенной информационно-логической вычислительной системой 35 согласуется с кодовой таблицей защищенного арифметического процессора 34. Для этого вместо исходного числового кода во входной столбец кодовой таблицы арифметического процессора 34 записывается содержимое одного из регистров столбцов блока регистров столбцов 79-1, 79-2,...,79-n многоалфавитного кодера второй ступени 101 стохастического преобразования. При этом во втором выходном столбце кодовой таблицы защищенного арифметического процессора 34 содержатся стохастические индексы числовых данных, используемые при выполнении

вычислений в защищенном виде. В процессе перекодирования последовательности кодовых блоков полученного сообщения во второй ступени 101 стохастического преобразования по сигналу блока 87 управления будет постоянно включен только один выбранный регистр. Поэтому полученная закрытая числовая информация будет перекодирована во входной код защищенного арифметического процессора 34 и по командам защищенной информационно-логической вычислительной системы 35 будет выдаваться через кодовую таблицу в защищенный арифметический процессор 34 для выполнения заданных вычислений. Полученные в результате вычислений данные в защищенном виде поступают через выходную кодовую таблицу для перекодирования из стохастических индексов защищенного арифметического процессора 34 во внутренний стохастический код. Для этого в выходной столбец обратной кодовой таблицы, входной столбец которой содержит индексы числовых данных, по сигналу блока управления 30 защищенной обработкой записывается содержимое одного из регистров столбцов многоалфавитного кодера блока индексации стохастического кода. В процессе перекодирования последовательности кодовых блоков полученного результата в первой ступени 98 стохастического преобразования по сигналу блока 87 управления будет постоянно включен только один выбранный регистр. Поэтому полученная закрытая числовая информация будет перекодирована в стохастический внутренний код и выдана по командам блока управления 30 защищенной обработкой в устройство 27 стохастического перекодирования, которое относится к типу «внутренний код - внешний код», для передачи в защищенном виде в пользовательское устройство 2.

Если в блоке управления 30 защищенной обработкой по формату сообщения определено, что тип обработки полученной закодированной информации - поиск и выборка по условию запроса требуемой информации из защищенных таблиц 39 данных, то подключается защищенная информационно-логическая вычислительная система 35. Она принимает зашифрованную информацию, которая может содержать:названия таблиц, их записей или полей, числовые параметры (им должны соответствовать выбираемые данные), коды арифметических вычислений (их необходимо произвести с выбранными числовыми полями).

При обработке запроса в защищенную информационно-логическую вычислительную систему 35 из защищенной базы данных 36 считывается последовательность кодовых блоков, содержащая зашифрованные имена таблиц, в начале которых содержатся зашифрованные комбинации и многочлены рекуррентного регистра внутреннего кода. Затем туда поступают соответствующие открытые ключи. После этого путем применения описанных выше процедур перекодирования и сравнения информации в защищенном виде производится выборка из зашифрованной последовательности кодов таблиц, необходимых для обработки запроса, который получен от пользовательского устройства 2. При этом каждый код с именем таблицы поочередно перекодируется с использованием соответствующих комбинаций рекуррентных регистров в первой 98 и второй 101 ступенях стохастического преобразования во внутренний код защищенной базы данных 36, которым зашифровано каждое из имен защищенных таблиц данных 39. При совпадении сравниваемых значений необходимые защищенные таблицы данных 39 по их коду считываются из защищенной базы данных 36 в защищенную информационно-логическую вычислительную систему 35 для дальнейшей обработки.

В процессе обработки учитывается, что каждая из записей (строк) защищенных таблиц данных 39 содержит последовательность кодовых блоков. При этом каждый кодовый блок соответствует определенному полю, код которого содержится в заголовке таблицы. В служебном поле имеется комбинация рекуррентного регистра для заголовка таблицы и каждой ее записи. В устройстве стохастического перекодирования 29 с использованием соответствующих комбинаций рекуррентных регистров производится перевод кодов полей, указанных в запросе, во внутренний код, которым зашифрованы коды полей в заголовке таблицы, и их сравнение. При совпадении сравниваемых значений из записей таблицы выбираются кодовые блоки указанных в запросе полей.

Если необходимо выбрать определенные данные или числовые параметры полей в зашифрованном виде в соответствии с кодами запроса из таблицы, то производится перекодирование кодов запроса во внутренний код каждой записи для выбора необходимых защищенных данных путем их сравнения с кодами запроса. Это реализуется описанным выше порядком с использованием комбинаций рекуррентных регистров в служебных полях записей. Если при сравнении числовых параметров используются арифметические операторы «больше» или «меньше», которые реализуются путем вычитания защищенных чисел, а также необходимо выполнить арифметические вычисления с выбранными полями в зашифрованном виде, то к процессу обработки подключается защищенный арифметически процессор 34. При этом вычисления с защищенной информацией реализуются описанным выше порядком. После завершения процесса обработки запроса выбранные из защищенных таблиц 39 закодированные данные или полученные результаты вычислений переводятся в устройстве стохастического перекодирования 29 во внутренний код сервера 3 распределенной обработки и описанным выше порядком передаются в пользовательское устройство 2.

Если в блоке управления 30 защищенной обработкой по формату сообщения определено, что тип обработки полученной закодированной информации - поиск и выборка по условию запроса защищенных Web-страниц 38, то подключается защищенная информационно-логическая вычислительная система 35. При этом реализуется два уровня поиска: первый уровень - по заголовкам защищенных Web-страниц 38, второй - по их содержанию. Поэтому при кодировании защищенных Web-страниц 38 используются два внутренних стохастических кода: первый код - для кодирования заголовка, второй - для защиты содержания самой страницы. При этом в начале каждой кодовой последовательности размещается служебный блок с комбинацией рекуррентного регистра. Полученное закрытое сообщение с условиями запроса имеет набор кодов ключевых слов, которые должны содержаться в запрашиваемом документе.

При поиске на первом уровне коды ключевых слов поступают в устройство стохастического перекодирования 29, переводятся во внутренний код заголовка очередной защищенной Web-страницы 38. При этом код каждого ключевого слова поочередно сравнивается с каждым кодовым блоком заголовка. В случае несовпадения сравниваемых кодов в них выделяется закодированная основа слова путем отбрасывания кодовых символов его окончания и производится повторное сравнение полученных кодов. В случае совпадения сравниваемых значений фиксируется наличие данного ключевого слова в заголовке. При несовпадении кодов ключевых слов с кодами заголовка переходят к следующей Web-странице, и т.д. Отобранные в результате поиска закодированные заголовки защищенных Web-страниц 38 преобразуются в устройстве 27 стохастического перекодирования сервера 3 распределенной обработки во внешний код и передаются по компьютерной системе в пользовательское устройство 2. Там после получения кодовых блоков производится их перекодирование во внутренний код, передача по шинам компьютера во внутренний стохастический декодер 14 и выдача в открытом виде запрашиваемой информации на экран монитора. При выборе определенной Web-страницы пользователь вводит запрос на ее получение из сервера 3 распределенной обработки данных. После выполнения описанных выше функций стохастического кодирования и перекодирования запроса в пользовательском устройстве 2 происходит передача защищенной информации по компьютерной системе. В результате запрос поступает в сервер 3 распределенной обработки, где выполняются функции его перекодирования, выбора требуемой защищенной Web-страницы 38 и передачи в пользовательское устройство 2.

Если поиск требуемой Web-страницы на первом уровне не дал результатов, то по запросу пользователя может быть произведен поиск ключевых слов непосредственно в тексте тех защищенных Web-страниц 38, в заголовке которых содержится хотя бы одно ключевое слово запроса. При этом используется описанная выше процедура перекодирования ключевых слов, их сравнение с кодами слов текста и кодами основ слов.

При наличии определенного числа совпадений каждого из ключевых слов запроса с кодами текста считается, что данная защищенная Web-страница 38 отвечает условиям запроса и передается в зашифрованном виде с использованием функций перекодирования в пользовательское устройство 2.

Промышленная применимость

Заявленные способ и система могут найти широкое применение в компьютерных системах, использующих распределенную обработку конфиденциальной информации. К ним можно отнести современные банковские и платежные системы, системы электронной почты с защитой информации, корпоративные сети и другие системы подобного типа.

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 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 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 личного ключа.

18. Способ по п.16 или 17, отличающийся тем, что аутентификации отправителя и контроля целостности принятой информации с помощью значения хэш-функции и электронной цифровой подписи используют секретный личный ключ 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) 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 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).

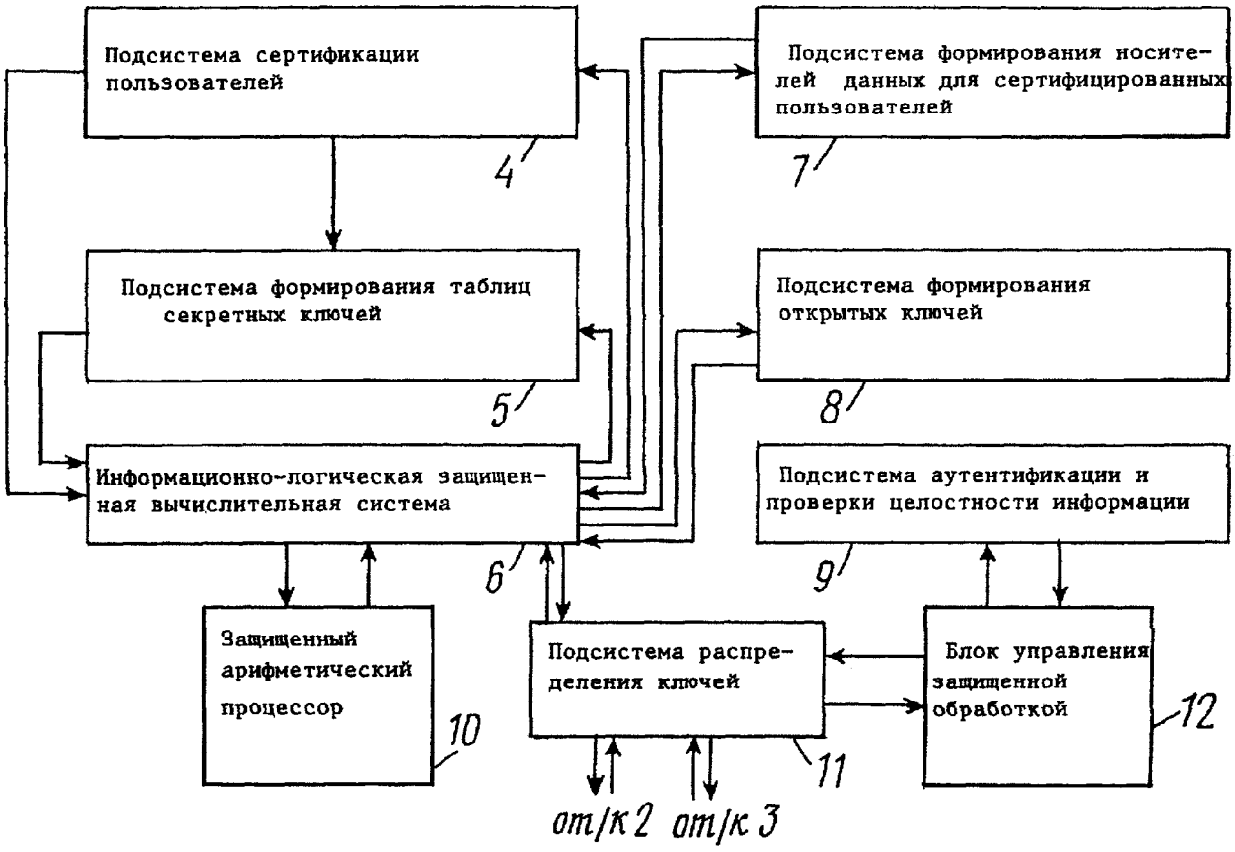
26. Стохастический кодер для системы комплексной защиты распределенной обработки информации, содержащий входной регистр перестановки (78), вход которого является входом кодируемых данных стохастического кодера, блок регистров столбцов многоалфавитного кодера (79-1,...,79-n), первым входом соединенный 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, 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.

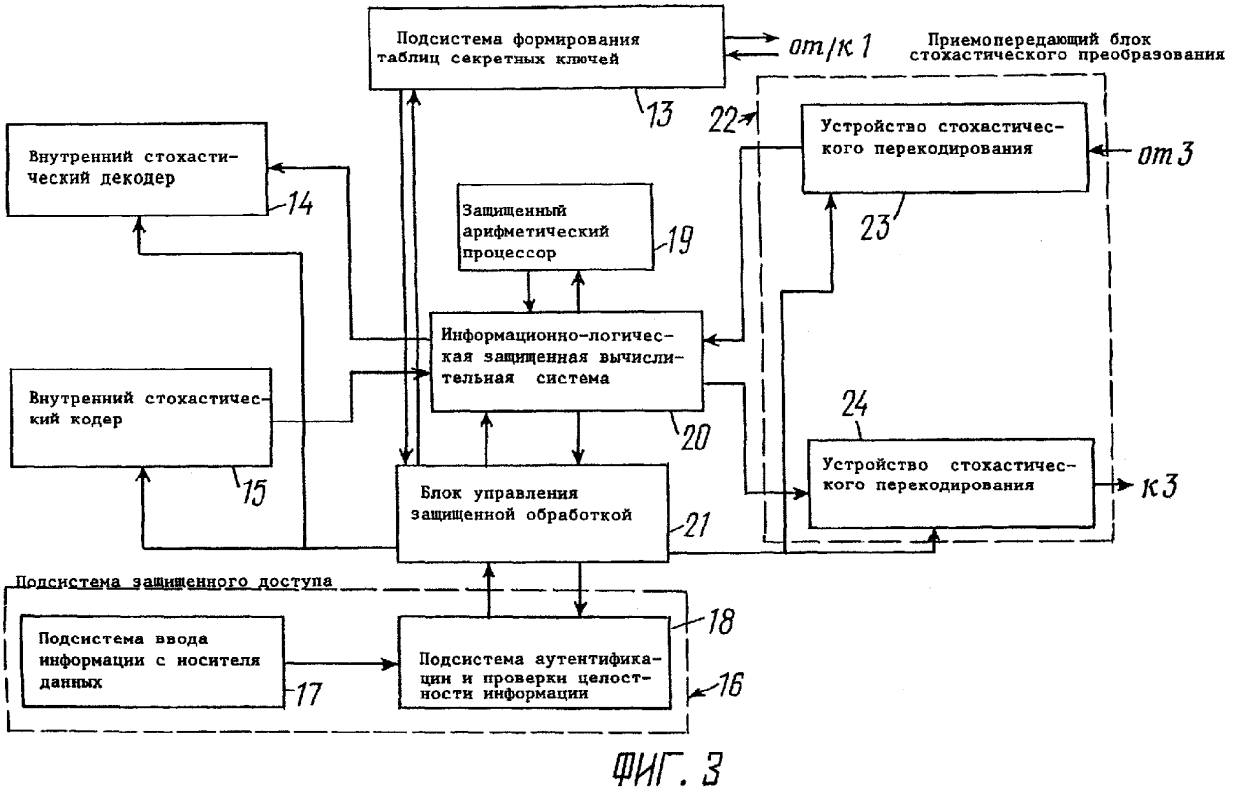
27. Стохастический кодер по п.26, отличающийся тем, что схема формирования гаммы (84) содержит блок регистров столбцов таблицы формирования гаммы (88-1,...,88-n), схему подключения столбцов (89), выходами соединенную со входами блока регистров столбцов таблицы формирования гаммы (88-1,...,88-n), циклический 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, 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 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-

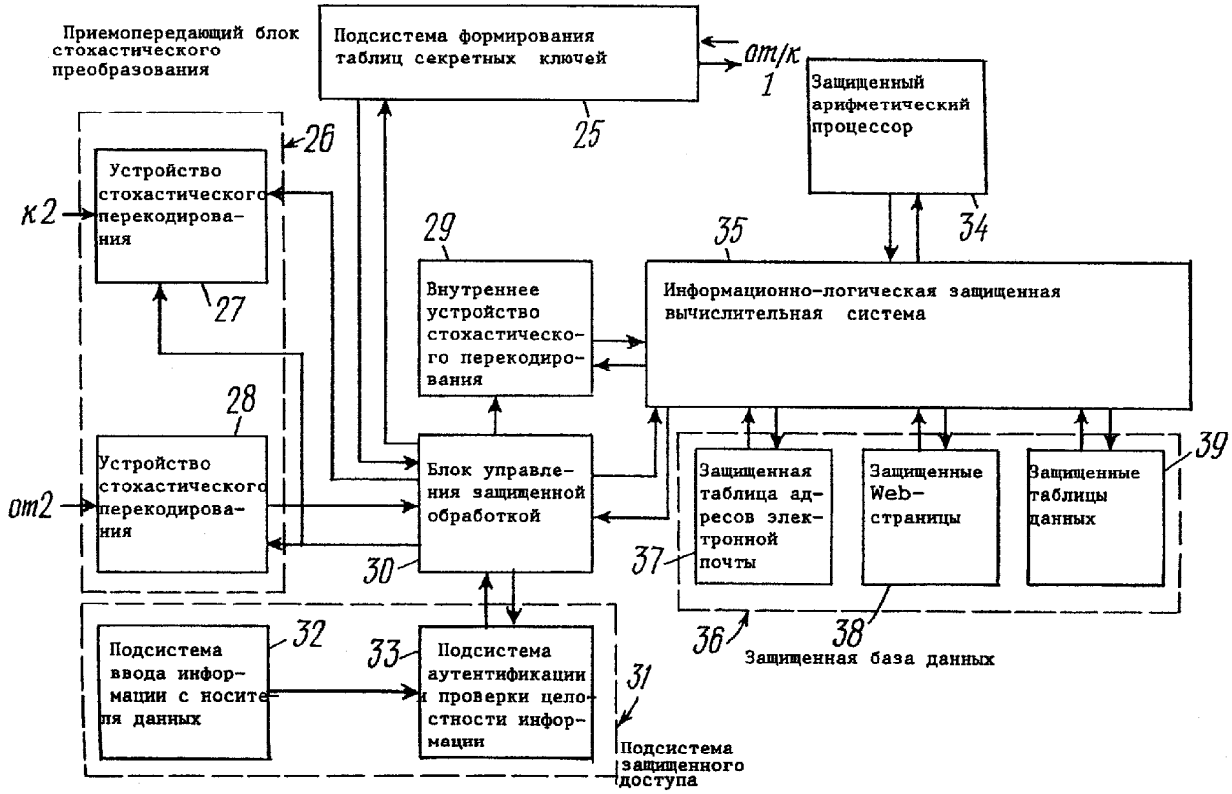
1,...,79-n), циклический регистр перестановки (81), выходами соединенный с соответствующими входами схемы подключения столбцов (80), блок ключей-инверторов (82-1,...,82-n), выходы которого соединены с соответствующими входами циклического регистра перестановки (81), рекуррентный регистр (83), выходами 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.


Подсистема сертификации пользователей
4
Подсистема формирования носителей данных для сертифицированных пользователей
7
Подсистема формирования таблиц секретных ключей
5
Подсистема формирования открытых ключей
8
Информационно-логическая защищенная вычислительная система
6
Подсистема аутентификации и проверки целостности информации
9
Защищенный арифметический процессор
10
Подсистема распределения ключей
11
Блок управления защищенной обработкой
12
от/к 2
от/к 3

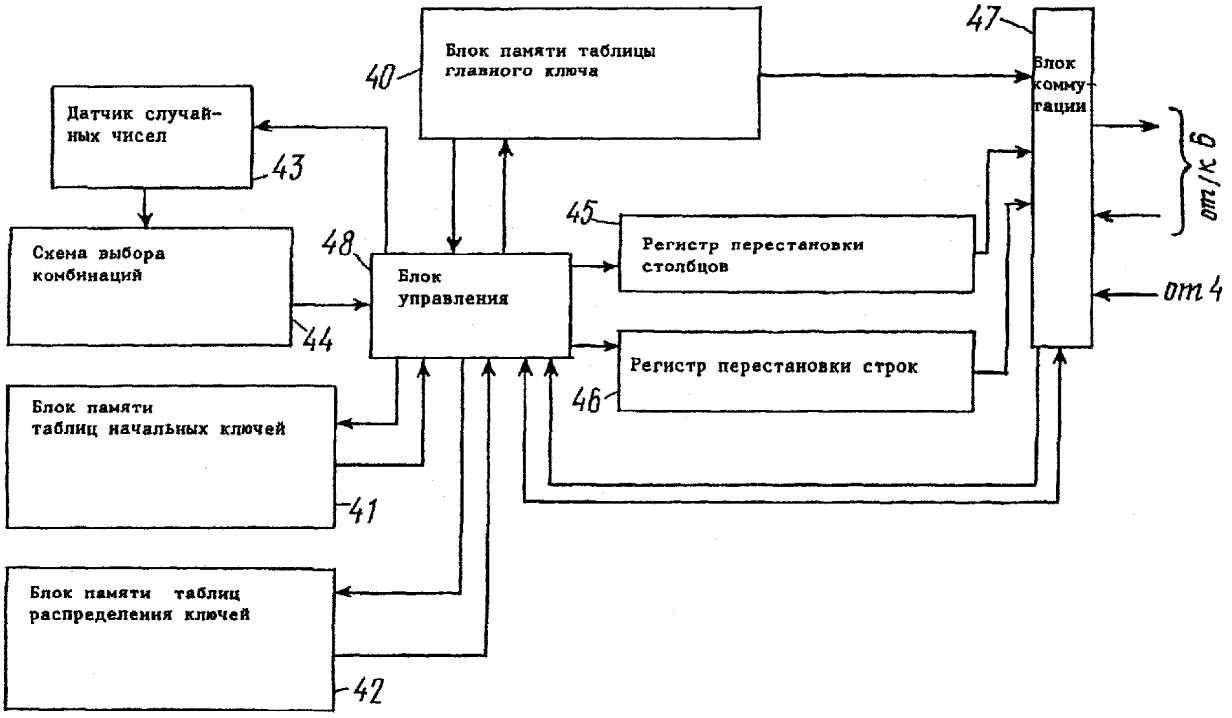
ФИГ. 2


Подсистема формирования таблиц секретных ключей
13
от/к 1
Приемопередающий блок стохастического преобразования
22
Устройство стохастического перекодирования
23
от 3
Внутренний стохастический декодер
14
Защищенный арифметический процессор
19
Информационно-логическая защищенная вычислительная система
20
Внутренний стохастический кодер
15
24
Устройство стохастического перекодирования
к 3
Блок управления защищенной обработкой
21
Подсистема защищенного доступа
Подсистема ввода информации с носителя данных
17
Подсистема аутентификации и проверки целостности информации
16
18

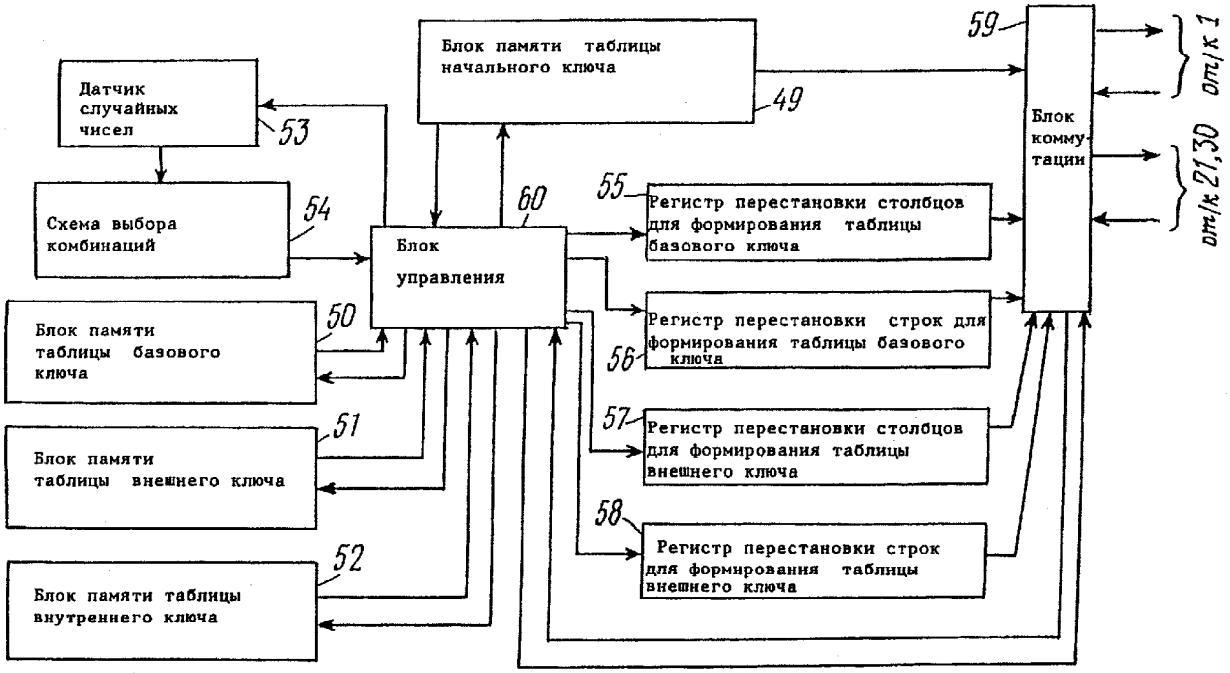
ФИГ. 3


Приемопередающий блок стохастического преобразования
Подсистема формирования таблиц секретных ключей
от/к 1
Защищенный арифметический процессор
25
26
Устройство стохастического перекодирования
к2
27
29
Внутреннее устройство стохастического перекодирования
35
Информационно-логическая защищенная вычислительная система
34
28
Устройство стохастического перекодирования
от2
Блок управления защищенной обработкой
30
Защищенная таблица адресов электронной почты
Защищенные Web-страницы
Защищенные таблицы данных
39
37
36
38
Защищенная база данных
Подсистема ввода информации с носителя данных
32
33
Подсистема аутентификации и проверки целостности информации
31
Подсистема защищенного доступа

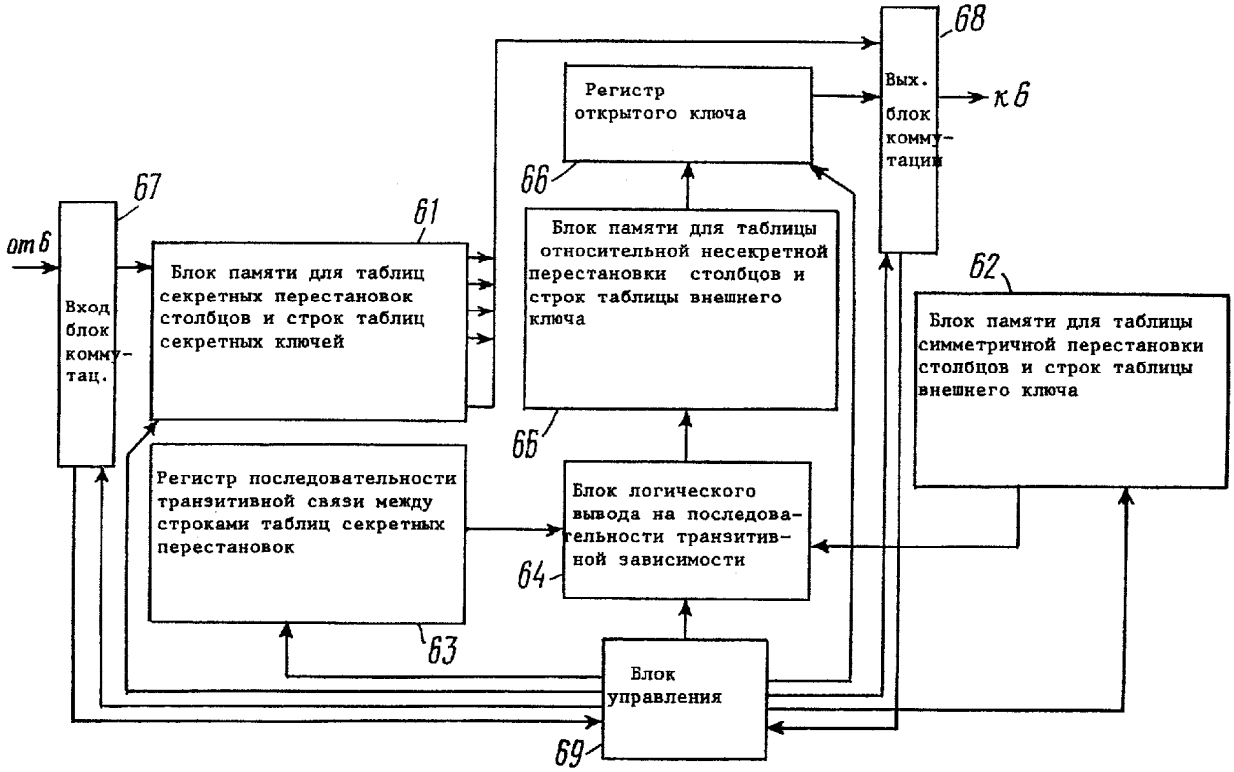
ФИГ. 4


Блок памяти таблицы главного ключа
40
47
Блок коммутации
Датчик случайных чисел
43
6 от/к
Схема выбора комбинаций
48
Блок управления
45
Регистр перестановки столбцов
от 4
44
Регистр перестановки строк
46
Блок памяти таблиц начальных ключей
41
Блок памяти таблиц распределения ключей
42

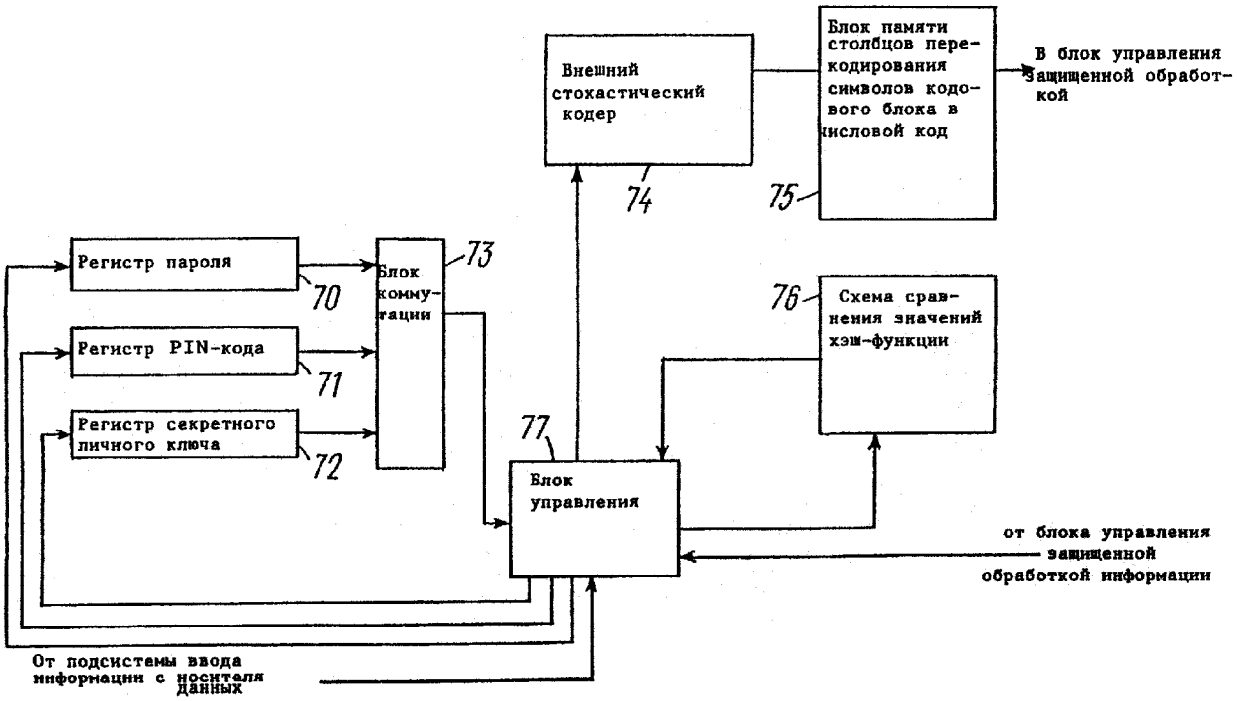
ФИГ. 5


Блок памяти таблицы начального ключа
49
59
Блок коммутации
от/к 1
от/к 21,30
Датчик случайных чисел
53
Схема выбора комбинаций
54
Блок управления
60
55
Регистр перестановки столбцов для формирования таблицы базового ключа
Регистр перестановки строк для формирования таблицы базового ключа
56
57
Регистр перестановки столбцов для формирования таблицы внешнего ключа
58
Регистр перестановки строк для формирования таблицы внешнего ключа
Блок памяти таблицы базового ключа
50
Блок памяти таблицы внешнего ключа
51
Блок памяти таблицы внутреннего ключа
52

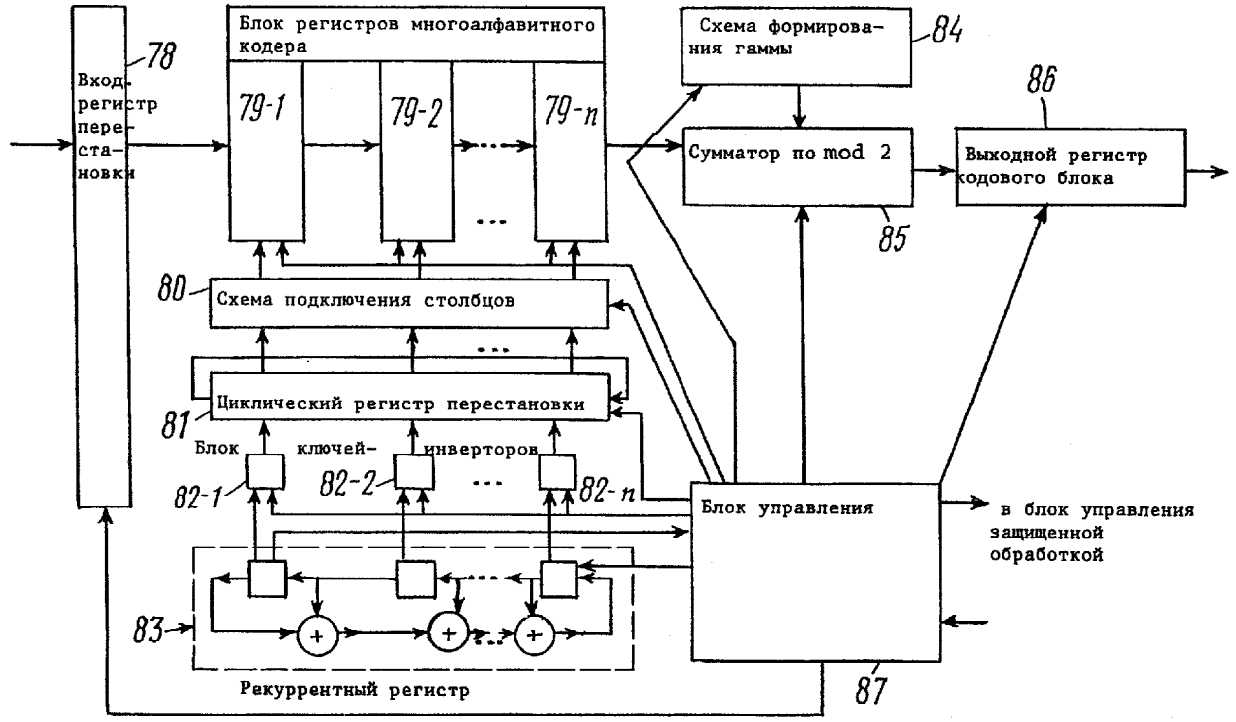
ФИГ. 6


68
Регистр открытого ключа
Вых. блок коммутации
к 6
66
67
от 6
Вход блок коммутац.
61
Блок памяти для таблиц секретных перестановок столбцов и строк таблиц секретных ключей
Блок памяти для таблицы относительной несекретной перестановки столбцов и строк таблицы внешнего ключа
65
62
Блок памяти для таблицы симметричной перестановки столбцов и строк таблицы внешнего ключа
Регистр последовательности транзитивной связи между строками таблиц секретных перестановок
63
Блок логического вывода на последовательности транзитивной зависимости
64
Блок управления
69

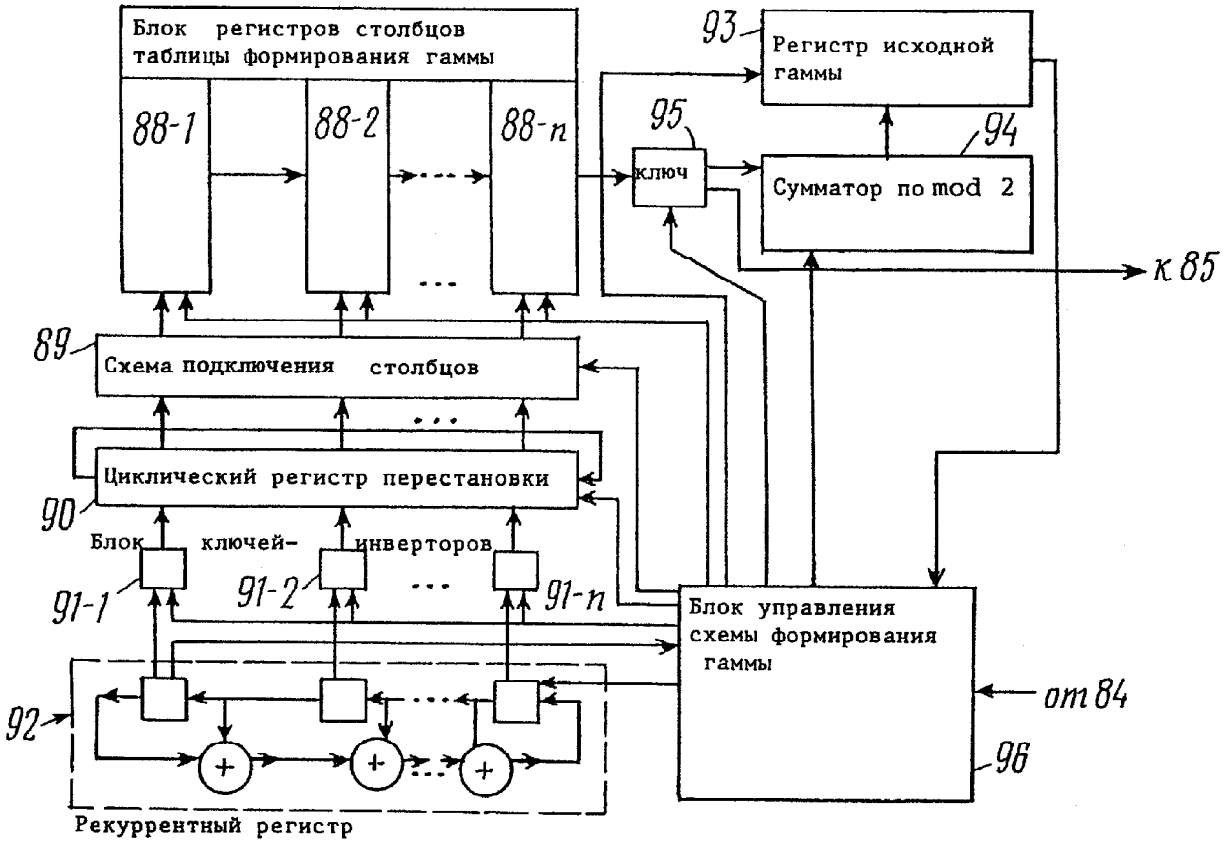
ФИГ. 7


Внешний стохастический кодер
74
Блок памяти столбцов перекодирования символов кодового блока в числовой код
75
В блок управления защищенной обработкой
Регистр пароля
70
Регистр PIN-кода
71
Регистр секретного личного ключа
72
Блок коммутации
73
76
Схема сравнения значений хэш-функции
77
Блок управления
от блока управления защищенной обработкой информации
От подсистемы ввода информации с носителя данных

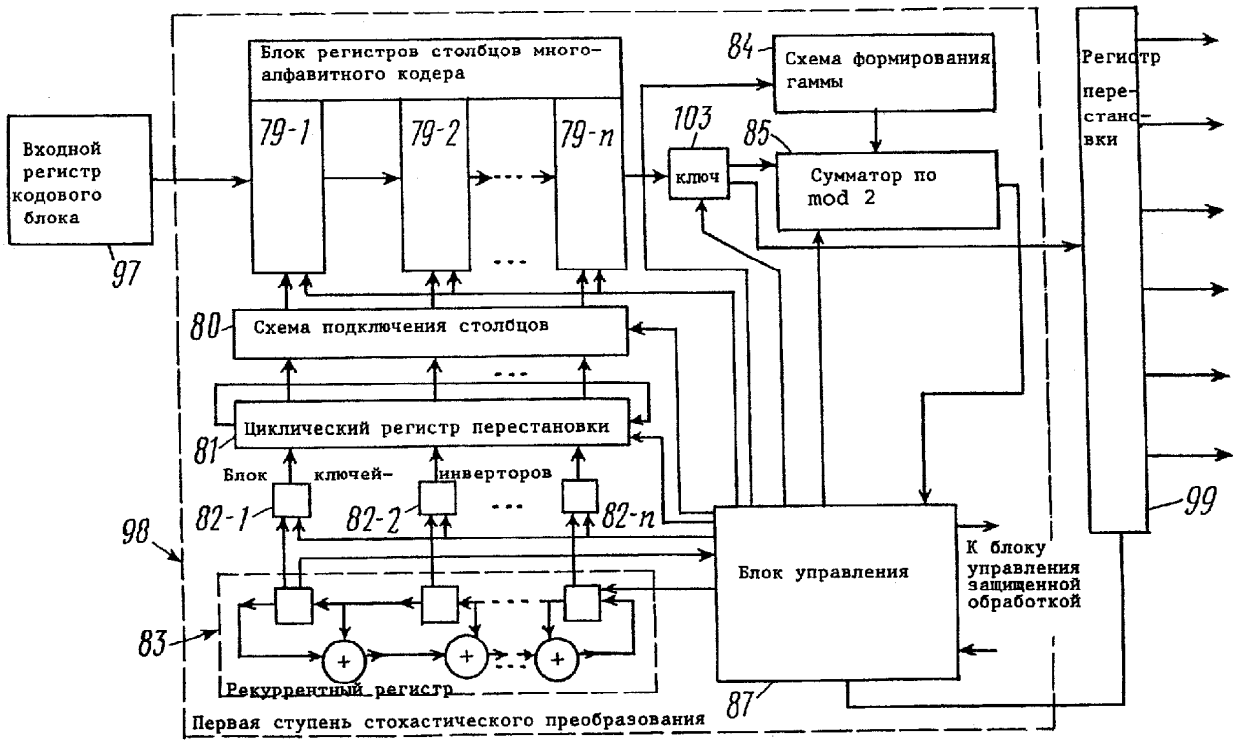
ФИГ. 8


78
Вход. регистр перестановки
Блок регистров многоалфавитного кодера
79-1
79-2
79-n
Схема формирования гаммы
84
86
Сумматор по mod 2
85
Выходной регистр кодового блока
80
Схема подключения столбцов
81
Циклический регистр перестановки
Блок ключей-инверторов
82-1
82-2
82-n
Блок управления
в блок управления защищенной обработкой
83
Рекуррентный регистр
87

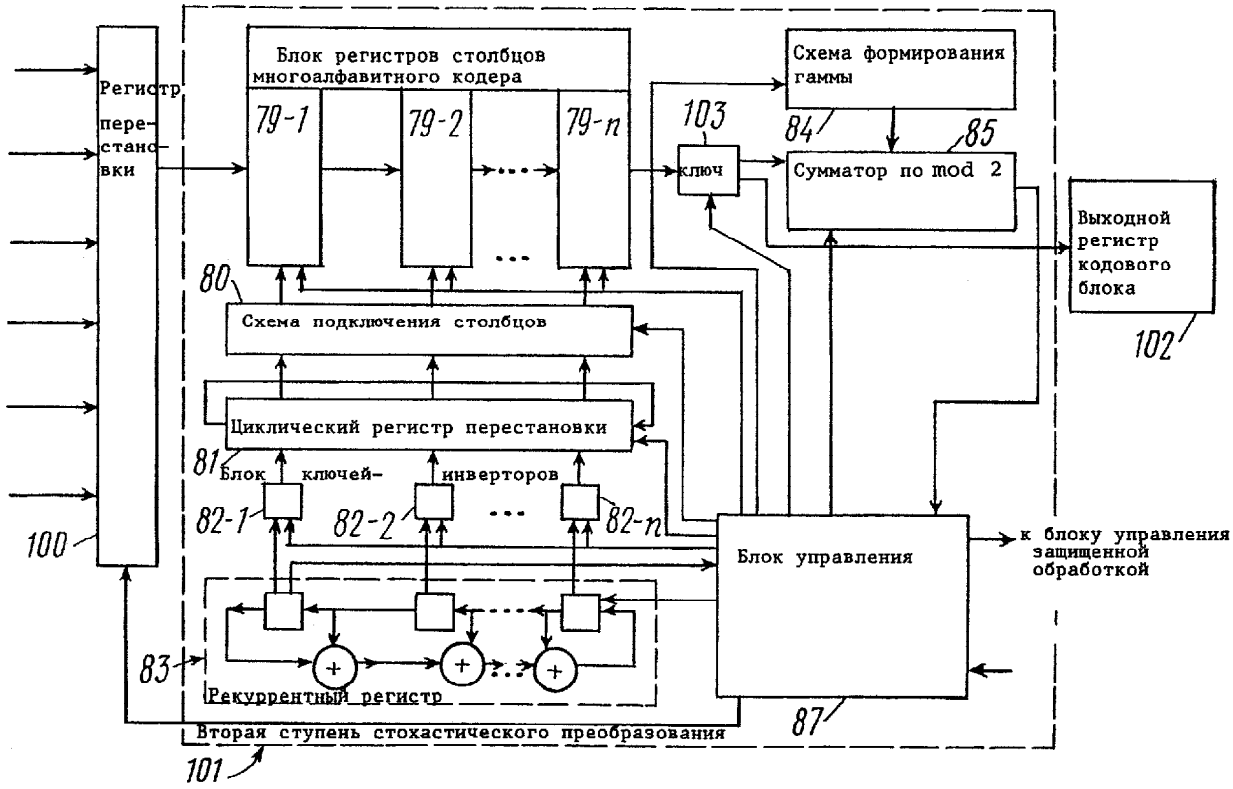
ФИГ. 9



ФИГ. 10



ФИГ. 11А

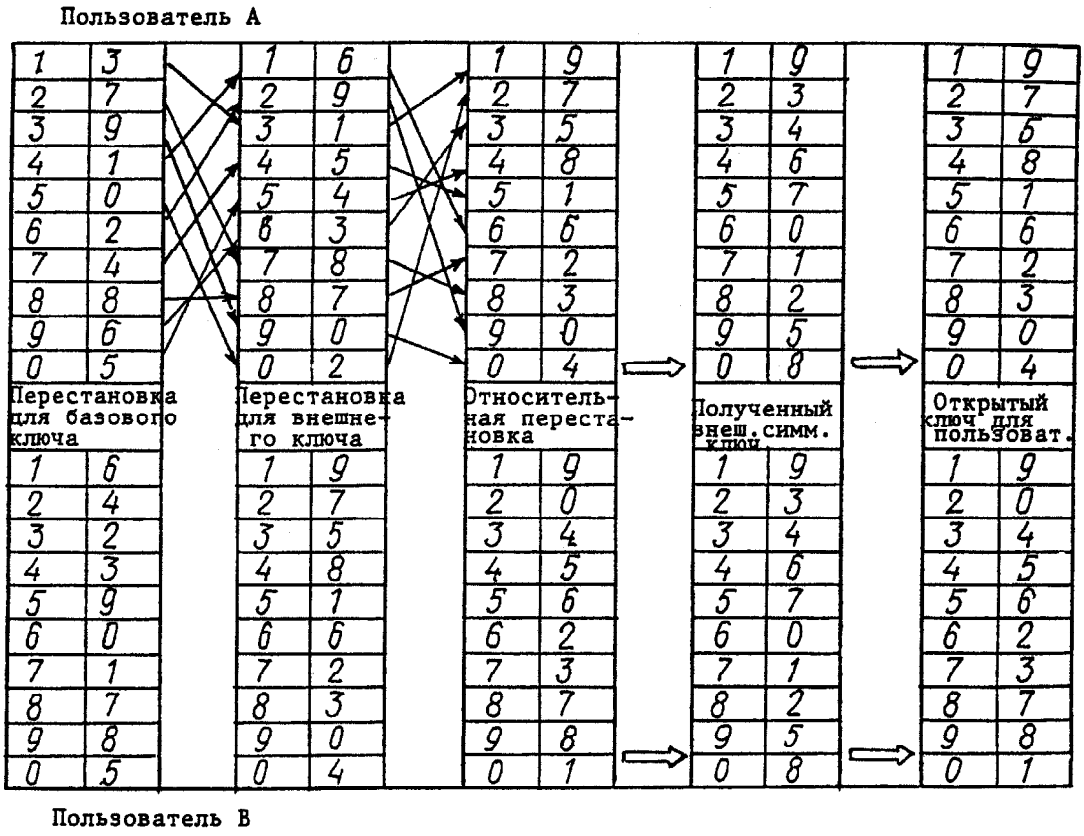


ФИГ. 11Б

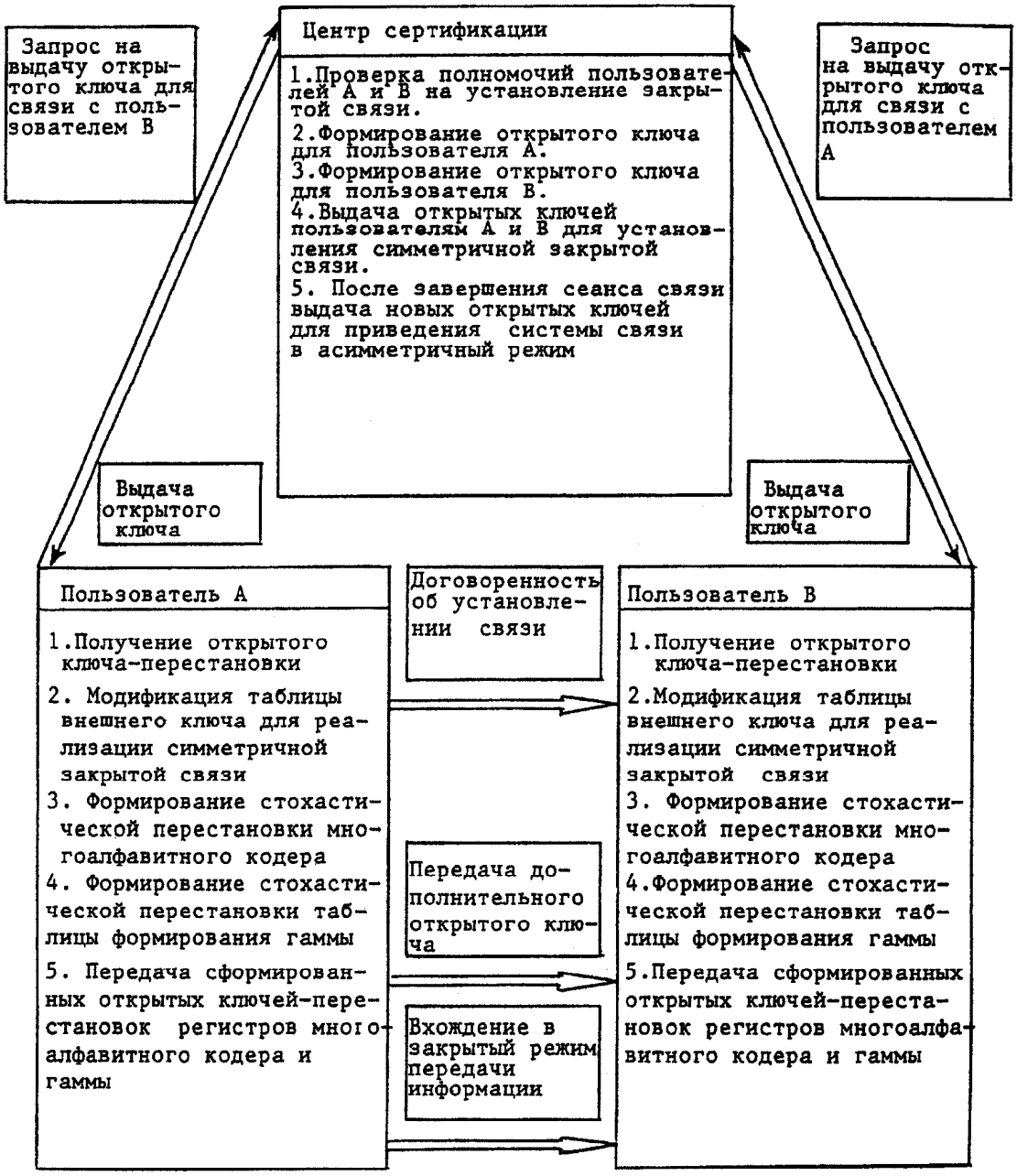
ТАБЛИЦА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ								
№ п/п	ФИО	Адрес ТЛФ	Паспортные данные	Пароль	Хэш-значение пароля	PIN-код	Ключевая перестановка столбцов	Ключев. перестановка строк

КОПИЯ СМАРТ-КАРТЫ ПОЛЬЗОВАТЕЛЯ						
Хэш-значение пароля	PIN-код	Перестановка столбцов для таблицы внешнего ключа	Перестановка строк для табл. внешнего ключа	Перестановка столбцов для базового ключа	Перестановка строк для базового ключа	Таблица начального ключа

ФИГ. 12


Пользователь А
Перестановка для базового ключа
Перестановка для внешнего ключа
Относительная перестановка
Полученный внеш.симм. ключ
Открытый ключ для пользоват.
Пользователь В

ФИГ. 13


Запрос на выдачу открытого ключа для связи с пользователем В
Центр сертификации
1.Проверка полномочий пользователей А и В на установление закрытой связи.
2.Формирование открытого ключа для пользователя А.
3.Формирование открытого ключа для пользователя В.
4.Выдача открытых ключей пользователям А и В для установления симметричной закрытой связи.
5. После завершения сеанса связи выдача новых открытых ключей для приведения системы связи в асимметричный режим
Запрос на выдачу открытого ключа для связи с пользователем А
Выдача открытого ключа
Выдача открытого ключа
Пользователь А
1.Получение открытого ключа-перестановки
2. Модификация таблицы внешнего ключа для реализации симметричной закрытой связи
3. Формирование стохастической перестановки многоалфавитного кодера
4. Формирование стохастической перестановки таблицы формирования гаммы
5. Передача сформированных открытых ключей-перестановок регистров многоалфавитного кодера и гаммы
Договоренность об установлении связи
Передача дополнительного открытого ключа
Вхождение в закрытый режим передачи информации
Пользователь В
1.Получение открытого ключа-перестановки
2.Модификация таблицы внешнего ключа для реализации симметричной закрытой связи
3. Формирование стохастической перестановки многоалфавитного кодера
4.Формирование стохастической перестановки таблицы формирования гаммы
5.Передача сформированных открытых ключей-перестановок регистров многоалфавитного кодера и гаммы

ФИГ. 14