РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 746 105**(13) **C2**

(51) МПК
G06F 21/12 (2013.01)
G06F 21/51 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/125 *(2020.08);* ***G06F 21/51*** *(2020.08);* ***G06F 8/30*** *(2020.08);* ***G06F 8/41*** *(2020.08);* ***G06F 8/61*** *(2020.08)*

(21)(22) Заявка: **2019103369, 07.02.2019**

(24) Дата начала отсчета срока действия патента:
07.02.2019

Дата регистрации:
07.04.2021

Приоритет(ы):
(22) Дата подачи заявки: **07.02.2019**

(43) Дата публикации заявки: **07.08.2020** Бюл. № 22

(45) Опубликовано: **07.04.2021** Бюл. № 10

Адрес для переписки:
125212, Москва, Ленинградское ш., 39а, стр. 3, АО "Лаборатория Касперского", Управление по интеллектуальной собственности, Московский Дмитрий Валерьевич

(72) Автор(ы):
Лукиян Дмитрий Сергеевич (RU),
Верещагин Алексей Георгиевич (RU)

(73) Патентообладатель(и):
Акционерное общество "Лаборатория Касперского" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2541935 C2, 20.05.2015. RU 2015125968 A, 10.01.2017. CN 108491197 A, 04.09.2018. US 2018/0121657 A1, 03.05.2018. US 2018/0115516 A1, 26.04.2018.**

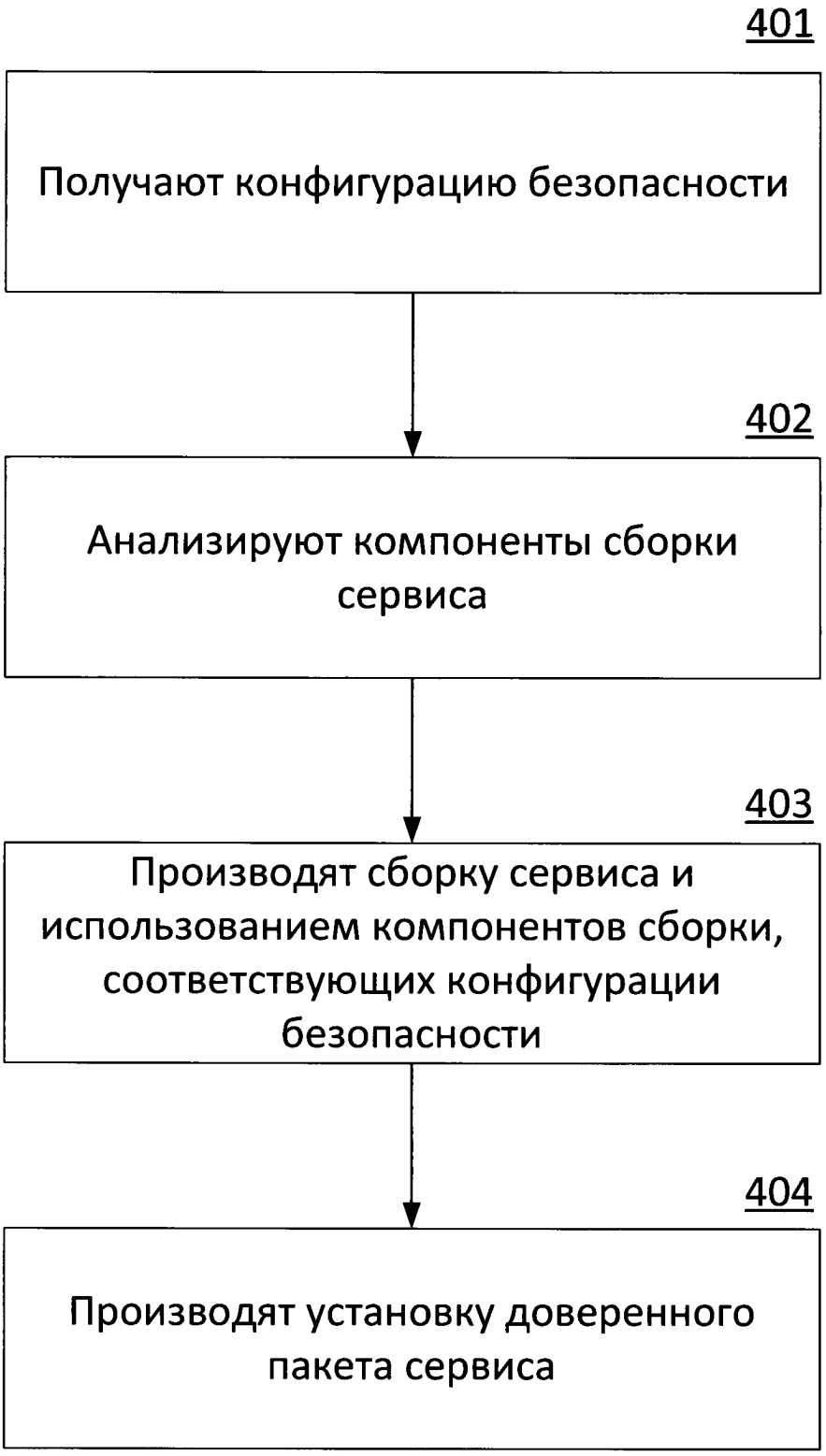
(54) Система и способ конфигурирования шлюза для защиты автоматизированных систем

(57) Реферат:

Изобретение относится к области защиты автоматизированных систем. Техническим результатом является обеспечение защиты устройств автоматизированных систем. Способ содержит этапы, на которых получают конфигурацию безопасности для приложения, которое предназначено для установки на вычислительное устройство автоматизированной системы; при этом конфигурация безопасности - это набор требований, предъявляемых к приложениям, выполнение которых обеспечивает требуемый уровень информационной безопасности автоматизированной системы; анализируют компоненты сборки приложения, предназначенного для установки на вычислительном устройстве автоматизированной системы, с целью проверки соответствия конфигурации безопасности; производят сборку приложения с использованием компонентов сборки, которые соответствуют конфигурации безопасности, в результате которой получают доверенный пакет приложения, при этом компонентом сборки является по меньшей мере файл исходного кода, а процесс сборки является компиляцией по меньшей мере одного файла исходного кода; производят установку приложения из доверенного пакета приложения на вычислительное устройство автоматизированной системы. 3 з.п. ф-лы, 5 ил.

RU 2746105 C2

RU 2746105 C2



Фиг. 4

RU 2746105 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 746 105**(13) **C2**

(51) Int. Cl.
G06F 21/12 (2013.01)
G06F 21/51 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/125 *(2020.08);* ***G06F 21/51*** *(2020.08);* ***G06F 8/30*** *(2020.08);* ***G06F 8/41*** *(2020.08);* ***G06F 8/61*** *(2020.08)*

(21)(22) Application: **2019103369, 07.02.2019**

(24) Effective date for property rights:
07.02.2019

Registration date:
07.04.2021

Priority:
(22) Date of filing: **07.02.2019**

(43) Application published: **07.08.2020** Bull. № **22**

(45) Date of publication: **07.04.2021** Bull. № **10**

Mail address:
125212, Moskva, Leningradskoe sh., 39a, str. 3, AO "Laboratoriya Kasperskogo", Upravlenie po intellektualnoj sobstvennosti, Moskovskij Dmitrij Valerevich

(72) Inventor(s):
Lukiyan Dmitrij Sergeevich (RU),
Vereshchagin Aleksej Georgievich (RU)

(73) Proprietor(s):
Aktsionernoe obshchestvo "Laboratoriya Kasperskogo" (RU)

RU 2746105 C2

(54) SYSTEM AND METHOD OF GATEWAY CONFIGURATION FOR AUTOMATED SYSTEMS PROTECTION

(57) Abstract:

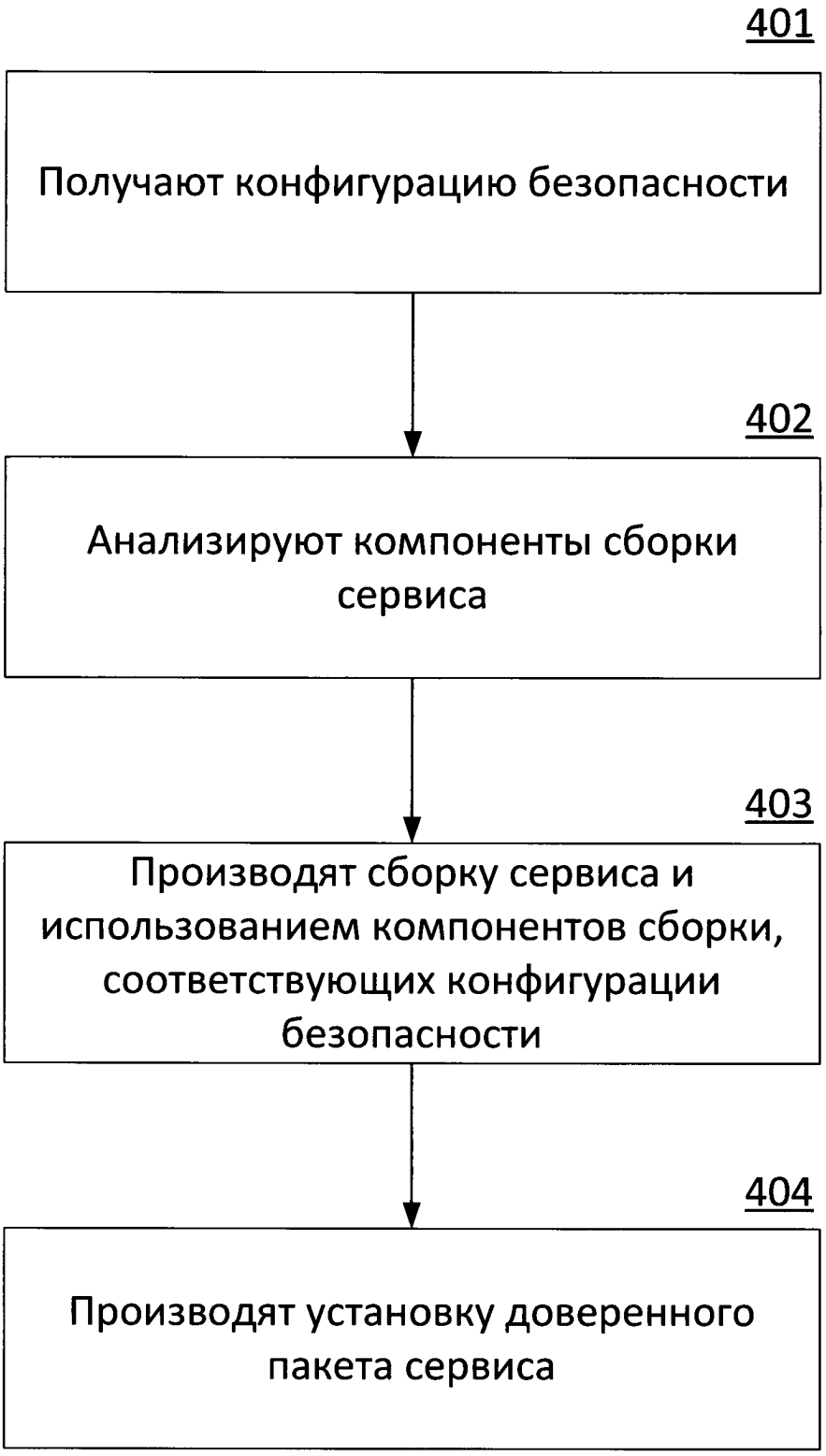
FIELD: electric communication technique.

SUBSTANCE: invention relates to the area of automated systems protection. The method consists of stages wherein the security configuration is procured for the application designed for installing an automated system onto a computing device, wherein the security configuration is a set of requirements for applications on meeting whereof a required level of data security of an automated system; the assembly components of the application designed for installing an automated system onto a computing device are analyzed to determine whether they comply with the security configuration; the application is assembled using assembly components that comply with the security configuration, resulting in a trusted application package, wherein the assembly component is no less than a source code file, and the assembly process is compiled of no less than one source code file; the application is installed from the trusted application package onto the computing device of the automated system.

EFFECT: technical result of the invention is ensured automated systems protection.

4 cl, 5 dwg

RU 2746105 C2



Фиг. 4

RU 2746105 C2

RU 2746105 C2

Область техники

Изобретение относится к области защиты автоматизированных систем.

Уровень техники

В современном мире все больше и больше электронных устройств подключаются к сети с целью удаленного управления ими или мониторинга. Такие устройства зачастую входят в состав АС (автоматизированных систем[1]) ([1]Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. ГОСТ 34.003-90.), а вид устройств варьируется от датчиков влажности дома до высокотехнологичных станков.

Как и любая сеть, сеть АС, соединяющая разнообразные устройства, является уязвимой к разного рода атакам со стороны злоумышленника. Примерами таких атак могут быть получение контроля над устройствами АС, например исполнительными элементами (приводами станков), или получение неправомерного доступа к данным относительно протекающих в АС технических процессов[2] ([2]ГОСТ 3.1109-82). Одним из способов защиты сети АС является создание приватной сети, доступ которой можно осуществить только с устройств, находящихся в физических пределах некоторой области. Однако полностью ограничить таим образом сеть АС - не лучшее решение, особенно, когда необходимо иметь удаленный доступ к некоторым потокам данных, формируемым устройствами АС.

Альтернативным решением проблемы защиты устройств в сети АС будет являться использование шлюза, который будет выполнять функцию «диода данных», т.е. будет позволять данным проходить только в одном направлении - от устройств АС в сегмент сети за пределами шлюза, но не наоборот.

В публикации GB 2558055 A, например, описана реализация такого «диода» при помощи нескольких шлюзов, один из которых является пограничным для сети АС, а другой обладает возможностью только передавать данные первому, но не принимать данные от него. Такая реализация «диода данных» обладает недостатком, связанным с сложностью конфигурирования такой схемы в случае внесения каких-либо изменений в конфигурацию безопасности - набора требований, соблюдение которых обеспечит требуемый уровень безопасности для устройств АС. Таким образом, необходим подход, который бы и защищал устройства АС, и позволял бы легко настраивать правила доступа к устройствам АС и используемые конфигурации безопасности.

Настоящее изобретение призвано преодолеть существующие недостатки известных подходов к защите сети АС и обеспечить безопасность устройств этой АС.

Раскрытие изобретения

Настоящее изобретение предназначено для обеспечения защиты устройств автоматизированных систем.

Технический результат изобретения заключается в реализации заявленного назначения.

Способ установки приложения, безопасный для устройств автоматизированной системы, согласно которому: получают конфигурацию безопасности для приложения, которое предназначено для установки на вычислительное устройство автоматизированной системы; при этом конфигурация безопасности - это набор требований, предъявляемых к приложениям, выполнение которых обеспечивает требуемый уровень информационной безопасности автоматизированной системы; анализируют компоненты сборки приложения, предназначенного для установки на вычислительном устройстве автоматизированной системы, с целью проверки соответствия конфигурации безопасности; производят сборку приложения с

использованием компонентов сборки, которые соответствуют конфигурации безопасности, в результате которой получают доверенный пакет приложения; производят установку приложения из доверенного пакета приложения на вычислительное устройство автоматизированной системы.

В другом варианте реализации способа вычислительным устройством автоматизированной системы является устройство, имеющее доступ как к ресурсам за пределами сети автоматизированной системы, так и устройствам самой автоматизированной системы.

В еще одном варианте реализации способа вычислительным устройством является шлюз, ограничивающий внутреннюю сеть автоматизированной системы.

В еще одном варианте реализации способа компонентом сборки является по меньшей мере файл исходного кода, а процесс сборки является компиляцией по меньшей мере одного файла исходного кода.

В еще одном варианте реализации способа на этапе анализа компонентов сборки собирается информация об известных уязвимостях компонентов, а также используемых структурах данных и вызываемых методах.

В еще одном варианте реализации способа на этапе анализа компонентов сборки компоненты сборки, не соответствующие конфигурации безопасности, изменяются с целью соответствия упомянутой конфигурации безопасности.

Краткое описание чертежей

Дополнительные цели, признаки и преимущества настоящего изобретения будут очевидными из прочтения последующего описания осуществления изобретения со ссылкой на прилагаемые чертежи, на которых:

Фиг. 1 иллюстрирует примерный вариант компонентов системы, реализующей настоящее изобретение.

Фиг. 2 иллюстрирует альтернативный вариант компонентов системы, реализующей настоящее изобретение.

Фиг. 3 показывает вариант реализации способа настоящего изобретения.

Фиг. 4 показывает альтернативный вариант реализации способа настоящего изобретения.

Фиг. 5 показывает пример компьютерной системы общего назначения.

Хотя изобретение может иметь различные модификации и альтернативные формы, характерные признаки, показанные в качестве примера на чертежах, будут описаны подробно. Следует понимать, однако, что цель описания заключается не в ограничении изобретения конкретным его воплощением. Наоборот, целью описания является охват всех изменений, модификаций, входящих в рамки данного изобретения, как это определено приложенной формуле.

Описание вариантов осуществления изобретения

Объекты и признаки настоящего изобретения, способы для достижения этих объектов и признаков станут очевидными посредством отсылки к примерным вариантам осуществления. Однако настоящее изобретение не ограничивается примерными вариантами осуществления, раскрытыми ниже, оно может воплощаться в различных видах. Сущность, приведенная в описании, является не чем иным, как конкретными деталями, необходимыми для помощи специалисту в области техники в исчерпывающем понимании изобретения, и настоящее изобретение определяется в объеме приложенной формулы.

Введем ряд определений и понятий, которые будут использоваться при описании вариантов осуществления изобретения.

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (ГОСТ 34.003-90). Примером автоматизированной системы может являться автоматизированная система управления (АСУ), в частности технологическими процессами (АСУ ТП), или же система датчиков и других устройств «умного дома» или других сетей, реализующих концепцию «интернета вещей» (англ. Internet of Things, IoT). В общем случае под АС будем понимать соединенные сетью устройства, доступ к которым извне должен быть строго регламентирован (в частности ограничен, например, доступом только «на чтение»), соответственно, настоящее изобретение предназначено для защиты комплекса средств автоматизации автоматизированной системы (ГОСТ 34.003-90), в частности устройств автоматизированной системы.

Шлюз безопасности (англ. security gateway), далее «шлюз» - точка соединения между сетями, между сегментами сетей или между программными приложениями в различных доменах безопасности, предназначенная для защиты сети в соответствии с существующей политикой безопасности (ГОСТ Р ИСО/МЭК 27033-1-2011). В рамках заявленного изобретения под шлюзом будем пониматься вычислительно устройство, соединяющее сегменты сетей, где одной из таких сетей является сеть, соединяющая устройства АС.

Конфигурация безопасности - это формализованный (например, в виде XML-файла) набор требований, предъявляемых к приложениям, выполнение которых обеспечивает требуемый уровень информационной безопасности автоматизированной системы. Конфигурация безопасности может являться частью политики безопасности.

Пакет прикладных программ (иногда «пакет приложений») - комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области. Примером пакета приложения может быть пакет сервиса (в понимании сервиса как приложения).

Сервис (иногда «служба», «демон», англ. daemon) - приложение, работающее в фоновом режиме.

Вредоносное приложение - приложение, способное нанести вред компьютеру или данным пользователя компьютера (иными словами, компьютерной системы), например: сетевой червь, клавиатурный шпион, компьютерный вирус. В качестве нанесенного вреда может выступать неправомерный доступ к ресурсам компьютера, в том числе к данным, хранящимся на компьютере, с целью хищения, а также неправомерное использование ресурсов, в том числе для хранения данных, проведения вычислений и т.п.

Доверенное приложение - приложение, которое не наносит вреда компьютеру или его пользователю. Доверенным приложением может считаться приложение, разработанное доверенным производителем ПО (программного обеспечения), загруженное из доверенного источника (например, сайт, занесенный в базу данных доверенных сайтов) или приложение, идентификатор (или другие данные, по которым можно однозначно определить приложение) которого (например, хеш-сумма файла приложения) хранится в базе данных доверенных приложений. Идентификатор производителя, например, цифровой сертификат, может также храниться в базе данных доверенных приложений. В одном из вариантов реализации доверенное приложение может быть установлено из доверенного пакета приложения.

Недоверенное приложение - приложение, которое не является доверенным, но также не признано вредоносным, например, при помощи антивирусного приложения. При этом недоверенное приложение может впоследствии быть признано вредоносным,

например, при помощи антивирусной проверки.

Вредоносный файл - файл, являющийся компонентом вредоносного приложения и содержащий программный код (исполняемый или интерпретируемый код).

Недоверенный файл - файл, являющийся компонентом недоверенного приложения и содержащий программный код (исполняемый или интерпретируемый код).

Доверенный файл - файл, являющийся компонентом доверенного приложения.

Под средствами системы защиты автоматизированных систем при помощи шлюза в настоящем изобретении понимаются реальные устройства, системы, компоненты, группы компонентов, реализованные с использованием аппаратных средств, таких как интегральные микросхемы (англ. application-specific integrated circuit, ASIC) или программируемые вентильные матрицы (англ. field-programmable gate array, FPGA) или, например, в виде комбинации программных и аппаратных средств, таких как микропроцессорная система и набор программных инструкций, а также на нейроморфных чипах (англ. neurosynaptic chips) Функциональность указанных средств системы может быть реализована исключительно аппаратными средствами, а также в виде комбинации, где часть функциональности средств системы реализована программными средствами, а часть аппаратными. В некоторых вариантах реализации часть средств, или все средства, могут быть исполнены на процессоре компьютера общего назначения (например, который изображен на Фиг. 5). При этом компоненты системы могут быть реализованы в рамках как одного вычислительного устройства, так и разнесены между несколькими, связанными между собой вычислительными устройствами.

Фиг. 1 отображает вариант системы защиты автоматизированных систем при помощи шлюза. Система, реализующая изобретение, включает в себя облачный сервис данных 104, средство управления 116, устройства автоматизированной системы 135, шлюз 105, функционирующий под управлением операционной системы (ОС) 120, а также приложения 130, которые функционируют в рамках шлюза 105.

Облачный сервис данных 104 представляет собой программно-аппаратный комплекс для предоставления информации, собираемой устройствами 135 автоматизированной системы. В еще одном варианте реализации изобретения облачный сервис данных 104 также может быть использован для управления устройствами 135 АС. Примером облачного сервиса данных 104 может являться Siemens MindSphere.

Примерами данных, которые предоставляются облачным сервисом 105 являются:

• статус работы устройства АС (включен/выключен или же находится в определенном состоянии обработки детали);

• положение инструмента устройства АС (положение в пространстве, углы наклона), осуществляющего воздействие на обрабатываемую деталь;

• время работы устройства АС с момента замена определенной детали (иными словами, износ детали);

• показания гигрометров;

• показания термометров;

• показания акселерометров;

• показания любы других датчиков, расположенных на устройствах АС.

Устройства 135 - устройства АС, которые могут как выполнять получаемые команды, так и предоставлять данные относительно функционирования - исполнительные механизмы, датчики, сенсоры. Для передачи данных между шлюзом 105 и устройствами 135 могут быть использованы различные протоколы передачи данных, например OPC UA или ModBus.

Примерами устройств 135 могут быть:

• датчик влажности;

• датчик освещенности;

• датчик давления (например, атмосферного);

• блок управления приводом (например, дверей, резцов, клапанов и т.п.);

• станок ЧПУ;

• двигатель;

• промышленный контроллер, например к которому подключены какие-либо датчики или сенсоры;

• любое другое устройство, используемое в промышленности или в качестве устройства умного дома, способное предоставлять информация и/или выполнять получаемые команды.

Средство управления 116 представляет собой вычислительное устройство, предназначенное для управления вычислительными устройствами АС, например, путем отправки команд. В одном из вариантов реализации изобретения средство управления 116 находится за пределами АС, и обмен данными между средством 116 и устройствами АС осуществляется через вычислительное устройство, имеющее доступ как к ресурсам за пределами сети АС, так и устройствам самой АС. Примером такого вычислительного устройства может являться шлюз 105, ограничивающий сеть АС (осуществляющий соединение сети АС и сети за пределами АС). Данный пример вычислительно устройства в качестве шлюза 105 будет далее использован для описания работы компонентов системы настоящего изобретения, не нарушая при этом общности упомянутого вычислительного устройства. При этом примерами управления, осуществляемого средством управления 116 в отношении устройств АС, может быть передача на устройство АС:

• пакетов программного обеспечения (например, сервисов);

• команды для установки пакетов программного обеспечения;

• конфигурации безопасности (а также параметры конфигурации, примеры которых будут приведены ниже);

• команды запуска/остановки работы.

Пример конфигурации безопасности, а именно требования, входящего в состав конфигурации безопасности, выглядит следующим образом (формализованный при помощи XML):

```
<constraint_list>
    <rule>
        <source type = TransmissionApp/>
        <action type = function_call,
        function_name = GetProcAddress,
        reaction = deny_function_call/>
    </rule>
</constraint-list>
```

Упомянутое требование запрещает приложению для передачи данных, например сервису передачи данных (TransmissionService), вызывать (deny_function_call) функцию GetProcAddress (function_name = GetProcAddress), иными словами требованием является отсутствие вызовов (или запрет вызовов) функции GetProcAddress со стороны приложения

для передачи данных.

Примерами требований в составе конфигурации безопасности могут также быть:

• отсутствие использования небезопасных структур данных;

• отсутствие использования небезопасных функций API;

• отсутствие использования исполняемого кода, например кода библиотек исполняемых файлов, относительно которого известно, что упомянутый код содержит уязвимости;

• отсутствие нарушений заданных политик безопасности;

• отсутствие доступа заданного приложения к данным (в том числе и предоставляемым другими приложениями, а также получаемым при помощи запросов, например SQL), к которым оно не должно иметь доступа в соответствии с моделью контроля доступа (например, Белла-Лападулы) или политикой безопасности;

• отсутствие вызовов функций, для которых заданы известные сигнатуры (описания функции), определяющие формат и размер допустимых параметров функции, с параметрами, которые не предусмотрены сигнатурой функции;

• отсутствие вызовов заданным приложением функций из закрепленного за этим приложением списка запрещенных функций (такие списки могут храниться в базе данных, связанной с сервисом безопасности 125).

Средство управления 116 также предназначено для:

• формирования конфигурации безопасности;

• сбора информации относительно архитектуры автоматизированной системы;

• анализа компонентов сборки приложений, предназначенных для исполнения на шлюзе 105, с целью проверки соответствия компонентов сборки приложений конфигурации безопасности;

• сборки приложения с использованием компонентов сборки приложения, в результате которой формируется пакет приложения.

При этом компонентами сборки являются данные, используемые для сборки пакета приложений. Такими данными являются по меньшей мере файлы исходного кода приложения. А процесс сборки представляет создание пакета приложения (англ. application package, программного пакета) из компонентов приложения, в частности компиляция исполняемых файлов приложения и последующая компоновка результатов компиляции.

Под архитектурой автоматизированной системы понимают информацию, описывающую совокупность аппаратного и программного обеспечения, функционирующего в рамках автоматизированной системы, такая информация содержит по крайней мере:

• список устройств с указанием назначения каждого из устройств;

• топология сетей автоматизированной системы, а также расположение шлюза, на который должно быть установлено приложение для передачи данных 110, относительно других устройств;

• список приложений, установленных на шлюзе, с указанием назначения каждого из приложений;

• список известных уязвимостей для каждого приложения, установленного на шлюзе;

• список протоколов обмена данных (Modbus, OPC UA и др.), с которыми работает каждое из установленных на шлюзе приложений, а также информация об известных уязвимостях протоколов передачи данных.

В одном из вариантов реализации изобретения средство управления 116 учитывает архитектуру АС при формировании конфигурации безопасности, такой учет архитектуры

автоматизированной системы для формирования конфигурации безопасности по меньшей мере обеспечивает защиту устройств автоматизированной системы от вредоносных действий, которые могут быть осуществлены от имени приложения, например, в случае компрометации приложения. Примером компрометации приложения, в частности приложения для передачи данных 110, может быть неправомерное получение удаленного доступа к выполнению кода от имени приложения 110 (иными словами, посредством исполнения кода из адресного пространства запущенного приложения 110).

Примерами учета архитектуры АС при формировании конфигурации безопасности могут являться:

• добавление в конфигурацию безопасности требования вида «отсутствие вызовов функции для получения указателя на функцию из библиотеки со стороны приложения» для каждого приложения, назначением которого является передача данных от устройств 135 АС, например за пределы сети АС, примером упомянутой функции является GetProcAddress;

• добавление в конфигурацию безопасности требования вида «отсутствие вызовов функции загрузки исполняемого кода в адресное пространство процесса со стороны приложения» для каждого приложения, назначением которого является передача данных, например за пределы сети АС, примером упомянутой функции является LoadLibrary;

• добавление в конфигурацию безопасности требования вида «отсутствие вызовов функций управления устройствами со стороны приложения», если назначение приложения - передача данных, а назначение устройства не ограничено сбором и предоставлением данных.

• добавление в конфигурацию безопасности требование вида «отсутствие передачи данных по протоколу передачи данных, формат которых не соответствует заданной сигнатуре», если приложение работает с протоколом, относительно которого известно о наличии уязвимостей (примером сигнатуры может быть формат пакета, размер которого не превышает заданное количество байт, например 128).

Стоит понимать, что вышеперечисленные примеры - варианты использования информации об архитектуре АС с одной целью - ограничить приложения, а именно их возможность выполнять действия, с помощью которых, например, может быть получен неправомерный доступ к ресурсам АС, в частности к устройствам АС.

Для выполнения вышеупомянутых функций средством 116, а также устройствами 135 на шлюзе 105 установлены и функционируют соответствующие приложения:

• сервис управления 115 для получения данных и выполнения команд от средства управления 116;

• приложения 130 для получения данных от устройств 135 и предоставления этих данных потребителям данных (будем называть это обслуживанием устройств 135), например приложению для передачи данных 110, а также для предоставления доступной информации об архитектуре АС (например, назначение соответствующего устройства 135).

Как было упомянуто ранее, шлюз 105 функционирует под управлением ОС 120. В одном из вариантов реализации изобретения операционной системой 120 является микроядерная ОС. Такая ОС обрабатывает все функции межпроцессного взаимодействия (англ. inter process communication - IPC), вызываемые приложениями (в частности, сервисами) шлюза 105, и при помощи сервиса безопасности 125 осуществляет свои функции по защите приложений 130 (например, защищая доверенные приложения от

действий недоверенных или скомпрометированных приложений), и, соответственно, устройств 135. Такие «защищенные» ОС 120 известны из уровня техники[3] ([3]Патентная заявка RU 2015125968 A), детальное описание принципов работы такой ОС выходит за рамки описания настоящего изобретения. Защита приложений 130 (которая, соответственно, обеспечивает защиту устройств 135) осуществляется путем ограничения действий приложений, которые могут быть источниками вредоносной активности (в частности, как было упомянуто ранее, активности, связанной с неправомерным доступом к ресурсам АС). Под ограничением можно понимать запрет на выполнение функций межпроцессного взаимодействия. При этом ограничения действий приложений определяются конфигурацией безопасности, которая используется сервисом безопасности 125 для принятия решения, какие функции межпроцессного взаимодействия могут быть осуществлены, а какие - нет.

В одном из вариантов реализации настоящего изобретения приложения 130, функционирующие на шлюзе 105, предназначены для получения данных от устройств 135, например, по одному из промышленных протоколов передачи данных, в частности OPC UA или ModBus. Таким образом передача данных (например, о состоянии какого-то технического процесса, показания сенсора или датчика) от устройств 135 шлюзу 105, и, если это требуется, далее в облачный сервис данных 104, осуществляется при помощи приложений 130, каждый из которых обслуживает одно или несколько устройств 135.

Для передачи данных от шлюза 105 на облачный сервис данных 104 используется функционирующее на шлюзе приложение для передачи данных 110. Такие приложения для передачи данных 110 предоставляются, как правило, владельцами, разработчиками или администраторами облачных сервисов данных 104 в виде программных пакетов для установки на вычислительное устройство, в частности шлюз 105, которое при помощи приложения для передачи данных 110 осуществляет передачу данных от подключенных устройств 135 (при помощи приложения 130) в облачный сервис данных 104. В еще одном варианте реализации приложение для передачи данных 110 предоставляется в виде компонентов сборки. Облачный сервис данных 104 используется как средство агрегации и предоставления информации, получаемой от устройств 130. Примером использования такого облачного сервиса данных 104 может быть подключение к нему вычислительного устройства, которое располагается в доме пользователя (или пользователь носит его с собой, в случае, если это мобильное вычислительное устройство) и собирает информацию с разных датчиков - устройств «умного дома». После этого облачный сервис данных 104 предоставляет пользователю возможность удаленного отслеживания состояния (и иногда управления состояниями) устройств его дома, например с использованием смартфона.

Так как приложение для передачи данных 110 предоставляется третьей стороной (вышеописанные владельцы, разработчики или администраторы облачных сервисов данных 104) для установки на шлюз 105, не являясь доверенным, существует опасность того, что приложение 110 будет скомпрометировано, и, например используя его уязвимости, злоумышленник получит доступ к устройствам 135 АС, приложениям 130 шлюза 105 - иными словами к программно-аппаратному комплексу автоматизированный системы.

Для решения данной задачи применяется ОС 120, под управлением которой функционирует шлюз 105, совместно с сервисом безопасности 125, который на основании конфигурации безопасности принимает решение, какие функции межпроцессного взаимодействия блокировать, а какие - нет. В частности, такими функциями могут быть

функции для получения данных приложением для передачи данных 110 от приложений 130, подключенных к устройствам 135. Такие вызовы, как правило, безопасны для устройств 130 АС, и конфигурация безопасности не предписывает блокировать такие вызовы, так как они направлены непосредственно для выполнения задачи, связанной с передачей данных от устройств 130 облачному сервису 104. С другой стороны, другие действия (вызовы функций межпроцессного взаимодействия IPC) приложения для передачи данных 110, которые выходят за рамки конфигурации безопасности, будут заблокированы сервисом безопасности 125, таким образом, обеспечивая требуемый уровень безопасности (в частности, информационной безопасности) устройств 130 АС.

Требование микроядерной архитектуры для ОС 120 обусловлено необходимостью контролировать полностью взаимодействие функционирующих на шлюзе 105 приложений - приложения для передачи данных 110, сервиса управления 115 и других приложений 130.

На Фиг. 2 отображена альтернативная схема системы конфигурирования шлюза для защиты автоматизированных систем. Система включает средство управления 116, которое в свою очередь содержит средство сборки 220, вычислительное устройство, в качестве примера которого выступает шлюз 105, и на котором функционируют ОС 120. В одном из вариантов такой ОС 120 является микроядерная ОС, особенности которой приведены в описании Фиг. 1. В другом варианте реализации к ОС 120 не предъявляется особых архитектурных требований. В одном из вариантов реализации изобретения шлюз 105 так же, как и в описании Фиг. 1 соединяет устройства 130 и облачный сервис 104.

На шлюзе 105 функционирует сервис управления 115, который способен осуществлять установку пакетов приложений на вычислительное устройство, в частности шлюз 105. В одном из вариантов реализации такой пакет приложения предоставляется средством управления 116.

В одном из вариантов реализации изобретения средство управления 116 хранит пакеты приложений (сервисов), которые могут быть установлены на устройства АС, в частности на шлюз 105, например, в предназначенном для этого хранилище или базе данных (не отображено на Фиг.). Данные, например, предварительно загруженные с удаленного сервера, в такое хранилище могут быть записаны специалистом или же при помощи предназначенного для этого программного обеспечения. В одном из вариантов реализации изобретения такой сервер принадлежит и/или используется разработчиками соответствующего программного обеспечения, пакет которого хранится средством управления 116.

В еще одном варианте реализации средство управления 116 само способно формировать пакет приложения 210 (в частности пакет сервиса) с использованием компонентов сборки упомянутого приложения 226. В этом случае саму сборку осуществляет средство сборки 220, которое может являться как компонентом средства управления 116, так и самостоятельным средством, функционирующим удаленно. Полученный при помощи средства сборки 220 пакет приложения впоследствии может быть установлен средством управления 116 на шлюз 105 АС.

В одном из вариантов реализации средство сборки 220 также способно осуществлять анализ компонентов сборки 226 на предмет соответствия конфигурации безопасности 225. В данном случае конфигурация безопасности 225 может быть как сформирована средством 116, так и предоставлена специалистом в области информационной безопасности или другим сторонним сервисом, например формирующим в качестве услуги конфигурации безопасности. Результатом анализа компонента сборки 226

приложения является определение, соответствует (удовлетворяет) ли компонент сборки 226 конфигурации безопасности 225 или нет.

В одном из вариантов реализации изобретения средство сборки 220 для формирования пакета приложения 210 использует только те компоненты сборки 226, которые были проанализированы и соответствуют конфигурации безопасности 225 (как по отдельности, так и в совокупности с требованиями конфигурации безопасности, предъявляемыми к таким компонентам 226). В таком случае средство сборки 220 формирует доверенный пакет приложения. Иными словами, доверенный пакет приложения - пакет приложения, сформированный средством сборки 220 из компонентов сборки, соответствующих конфигурации безопасности.

Средство сборки 220 также способно изменять компоненты сборки, не соответствующие конфигурации безопасности 225, таким образом, чтобы эти компоненты соответствовали упомянутой конфигурации 225. В одном из вариантов реализации изобретения данный шаг является заключительным шагом, выполняемым средством сборки 220 при проведении анализа компонента сборки 226, если упомянутый компонент 226 не соответствуют конфигурации безопасности 225.

Для того, чтобы проверить соответствие компонента сборки 226 конфигурации безопасности 225, как упоминалось ранее, средство сборки осуществляет анализ. В рамках данного анализа средство сборки 220 может собирать следующую информацию относительно компонента сборки 226:

- информацию об уязвимостях (по крайней мере известных), содержащихся в компоненте сборки 226;
- информацию об используемых структурах данных;
- информацию об используемых функциях API и методах;
- информацию о протоколах передачи данных, используемых кодом компонентов сборки 226.

Для получения вышеописанной информации могут быть использованы любые известные из уровня техники способы обнаружения уязвимостей и определения используемых типов данных и функций.

При обнаружении несоответствия некоторого компонента сборки 226 конфигурации безопасности 225 средство сборки 220 осуществляет изменение (если это возможно) соответствующего компонента сборки 226. Для приведения такого компонента сборки 226 в соответствие с конфигурацией безопасности 225 средство сборки 220 может:

- при обнаружении уязвимостей в компоненте сборки 226 заменять компонент сборки 226 на аналогичный компонент более ранней версии, в которой отсутствуют уязвимости;
- при обнаружении в компоненте сборки 226 использования небезопасных структур данных заменять эти использования (обращения) на использование безопасных аналогов, например потокобезопасных (англ. thread safe) типов данных;
- при обнаружении в компоненте сборки 226 использования небезопасных функций API заменять эти использования (обращения) на использование безопасных аналогов, например заменяя вызовы функций scanf на scanf_s.

В одном из вариантов реализации конфигурация безопасности 225 содержит требование, согласно которому компоненты сборки 226 должны быть устойчивы к ROP-атакам (англ. return-oriented programming). В таком случае средство сборки 220 рассматривает каждый компонент сборки 226 как уязвимый к ROP-атакам, для реализации которых злоумышленник инициирует исполнение кода в исполняемом файла таким образом, чтобы выполнялись последовательности инструкций (в качестве которых могут быть интерпретированы последовательности байт исполняемого файла), на

которые злоумышленник передает управление, например, при помощи стека, и такая последовательность инструкций представляла бы собой исполняемый код, реализующий некоторую атаку. В таком случае для приведения такого компонента сборки 226 в соответствие с конфигурацией безопасности 225 средство сборки 220 может произвести обфускацию исходного кода таким образом, чтобы сформированный исполняемый файл не поддавался бы ROP-атаке: при использовании ROP-атаки принципиально знание злоумышленника о байтовом представлении исполняемого файла, так как именно байтовое представление анализируется для формирования ROP-цепочки инструкций, которая реализует атаку злоумышленника. И в случае обфускации такая атака будет неосуществима.

В еще одном варианте конфигурация безопасности 225 содержит требование, согласно которому компоненты сборки 226 не должны содержать уязвимостей, которые могут быть обнаружены при помощи фаззинга (англ. fuzzing, тестирование с целью обнаружения уязвимостей), в таком случае средство сборки 220 рассматривает каждый компонент сборки 226 как потенциально уязвимый (имеющий уязвимости в коде). И для приведения такого компонента сборки 226 в соответствие с конфигурацией безопасности 225 средство сборки 220 может произвести фаззинг, с целью последующего устранения найденных уязвимостей с использованием любого из известных в уровне техники подходов.

Измененный вышеописанным образом компонент сборки 226 может быть использован средством сборки 220 совместно с остальными компонентами безопасности 226, соответствующими конфигурации безопасности 225, для формирования доверенного пакета приложения 210. Такой пакет 210 может быть впоследствии передан средством управления 116 на вычислительное устройство АС, в частности шлюз 105. В одном из вариантов реализации таким доверенным пакетом приложения 220 является доверенный пакет приложения, например приложения для передачи данных 110, который предназначен для установки на шлюз 105.

В одном из вариантов реализации изобретения, доверенный пакет приложения 210 может формироваться средством сборки 220 с использованием компонентов сборки 226, которые не удовлетворяют конфигурации безопасности 225, в таком случае, чтобы такое приложение, будучи установленным, было безопасным для устройств 135 АС (не нанесло вреда устройствам АС), пакет приложения формируется из компонентов сборки 226, в который впоследствии добавляется набор требований конфигурации безопасности 225, которые нарушались компонентами сборки 226. После установки приложения из такого пакета 210 на вычислительное устройство, например шлюз 105, работа приложения ограничивается сервисом безопасности 125 в соответствии с набором требований конфигурации безопасности 225, добавленным в пакет приложения 210. Таким образом осуществляется установка приложения из пакета приложения 210 безопасным для устройств 135 АС способом. Иными словами, для формирования доверенного пакета приложения 210 используется не только компонент сборки 226, которые не удовлетворяет требованиям конфигурации безопасности 225, а тот же самый компонент 226 совместно с набором требований конфигурации безопасности 225, которым он не соответствует (будем считать компонент 226 соответствующим конфигурации безопасности 225, когда он используется для сборки пакета приложения 210 совместно с упомянутым набором требований конфигурации безопасности 225).

В одном из вариантов реализации пакет приложения 210 предназначен не для установки некоторого приложения, а обновления уже установленного, например на шлюз 105, приложения. В таком случае пакет приложения 210 может быть использован

как для замены исполняемого кода некоторого приложения, так и обновления набора требования конфигурации безопасности 225, которые при установке приложения передаются сервису безопасности 125 для обеспечения требуемого уровня безопасности устройств 135 АС.

На Фиг. 3 отображен вариант способа, реализующего настоящее изобретение.

На этапе 301 при помощи средства управления формируют конфигурацию безопасности, соблюдение требований которой обеспечивает требуемый уровень безопасности устройств автоматизированной системы. При этом конфигурация безопасности может быть сформирована средством управления 116 с учетом архитектуры автоматизированной системы так, чтобы обезопасить устройства и приложения, которые могут являться целями атак злоумышленников. Сформированная конфигурация безопасности используется на этапе 302 сервисом управления 115, который функционирует в рамках вычислительного устройства, в частности шлюза 105 автоматизированной системы, для установки приложения, которое способно обмениваться данными с вычислительными устройствами за пределами сети автоматизированной системы. В одном из вариантов реализации изобретения таким приложением является приложение для передачи данных 110, которое может взаимодействовать с облачным сервисом данных 104, например MindSphere. Использование конфигурации безопасности при установке приложения 110 позволяет сервису безопасности 125 операционной системы 120 контролировать и обеспечивать соблюдение приложением для передачи данных 110 конфигурации безопасности. После этого, на этапе 303, осуществляют передачу данных от устройств автоматизированной системы через шлюз 105, а именно функционирующее на нем приложение для передачи данных 110, облачному сервису данных 104 таким образом, что все действия приложения для передачи данных 110 контролируются сервисом безопасности 125, что обеспечивает безопасность устройств автоматизированной системы при передачи данных с использованием приложения для передачи данных 110 (которое предоставлено третьей стороной и не является доверенным приложением).

Существует вероятность, что приложение для передачи данных 110 будет подвергнуто атаке злоумышленников и будет скомпрометировано таким образом, чтобы выполнять команды злоумышленников. Соответственно, выполнение описанного способа позволяет достичь такого полезного эффекта, что приложение для передачи данных 110, которое предоставляется третьей стороной, как правило разработчиками/владельцами облачного сервиса данных 104, не являясь доверенным, не сможет выполнять действия (посредством вызовов функций и IPC), которые запрещены конфигурацией безопасности, которая учитывалась при установке упомянутого приложения 110, и, соответственно, будет обеспечена безопасность устройств 135 (и приложений 130) автоматизированной системы, так как даже скомпрометированное приложением для передачи данных 110 не сможет получить доступ к устройствам 135 АС, не предусмотренный конфигурацией безопасности. Именно эти особенности защиты устройств 135 АС при помощи шлюза 105 и реализуют принцип «диода» данных, позволяя данным изнутри передаваться на облачный сервис 104, при этом не позволяя командам извне, в частности переданным по каналам связи, соединяющим шлюз 105 и облачный сервис 104, влиять на устройства 135 АС.

На Фиг. 4 отображен еще один вариант способа, реализующего настоящее изобретение.

На этапе 401 средство управления 116 получает конфигурацию безопасности 225, соблюдение требований которой обеспечивает требуемый уровень безопасности

устройств автоматизированной системы. В одном из вариантов реализации изобретения такая конфигурация может быть создана самим средством 116, в другом варианте реализации она может быть предоставлена специалистом в области информационной безопасности. После этого, на этапе 402, средство сборки 220 осуществляет анализ компонентов сборки 226 приложения, которое необходимо установить на вычислительное устройство автоматизированной системы. В одном из вариантов реализации изобретения таким устройством является шлюз 105, а приложением - приложение для передачи данных 110, необходимое для того, чтобы информация, предоставляемая устройствами 135 автоматизированной системы, была бы доступна на облачном сервисе данных 104. В результате такого анализа относительно каждого из компонентов сборки 226 принимается решение средством сборки 220 - является ли компонент сборки 226 соответствующим конфигурации безопасности или нет.

В одном из вариантов реализации изобретения средство сборки 220 способно изменять компоненты сборки 226 некоторого приложения (например, приложения для передачи данных). Такой шаг может быть выполнен в отношении компонентов сборки 226, которые не признаны соответствующими конфигурации безопасности 225 на этапе анализа 402, с той целью, чтобы после внесенных изменений такие компоненты сборки 226 стали соответствовать конфигурации безопасности 225.

После этого, на этапе 403, средство сборки 220 формирует пакет приложения 210, в частности приложения для передачи данных 110. При этом в одном из вариантов реализации изобретения для формирования пакета 210 используются только те компоненты сборки 226, которые соответствуют конфигурации безопасности 225. Полученный таким образом доверенный пакет приложения на этапе 404 устанавливается сервисом управления 115, который функционирует на вычислительном устройстве, на которое устанавливается и упомянутый доверенный пакет приложения. В одном из вариантов реализации изобретения таким вычислительным устройством является шлюз 105, а приложением - приложение для передачи данных 110.

Если же изменить компонент сборки 226, который не соответствует конфигурации безопасности 225, таким образом, чтобы он соответствовал конфигурации безопасности 225, на этапе 402 невозможно, то в одном из вариантов реализации изобретения формируемый средством сборки пакет приложения 220 затем устанавливают на вычислительное устройство автоматизированной системы с учетом конфигурации безопасности 225, что позволяет обеспечить безопасность устройств 135 автоматизированной системы в условиях, когда на одном из вычислительных устройств АС установлено приложение, по меньшей мере один компонент сборки 226 которого не соответствует конфигурации безопасности 225.

Существует вероятность, что приложение, функционирующее на вычислительном устройстве АС, будет подвергнуто атаке злоумышленников и будет скомпрометировано таким образом, чтобы выполнять команды злоумышленников. При этом в соответствии с вышеупомянутым способом приложение или сервис, которое предоставляется в виде компонентов сборки 226, например, третьей стороной (в случае, если приложение - приложение для передачи данных 110, компоненты сборки 226, как правило, предоставляются разработчиками/владельцами облачного сервиса данных 104), будет установлено на вычислительное устройство АС таким образом, чтобы не иметь возможность выполнять действия (посредством вызовов функций и IPC) или использовать структуры данных, которые запрещены конфигурацией безопасности 225, что достигается путем формирования и последующей установки доверенного пакета приложения (или, например, пакета сервиса) 220, который формируется из

компонентов сборки 226, которые удовлетворяют конфигурации безопасности 225.

Следовательно, выполнение описанного способа позволяет достичь такого полезного эффекта, заключающегося в обеспечении безопасности устройств 135 (и приложений 130) автоматизированной системы, так как даже скомпрометированное приложение (в частности, приложение для передачи данных 110), установленное из доверенного пакета приложения 220, не сможет осуществлять действия, запрещенные конфигурацией безопасности 225 на этапе формирования пакета приложения 220.

Дополнительный технический результат, связанный с выполнением вышеописанного способа заключается в обеспечении безопасности устройств 135 АС за счет того, что устанавливаемые на вычислительное устройство приложения (например, приложение для передачи данных 110), будут скомпрометированы с меньшей вероятностью, так как, по меньшей мере, конфигурация безопасности 225 запрещает формирование пакета приложения 220 для дальнейшей установки на вычислительном устройстве, если компоненты сборки содержат уязвимости.

Фиг. 5 представляет пример компьютерной системы общего назначения, персональный компьютер или сервер 20, содержащий центральный процессор 21, системную память 22 и системную шину 23, которая содержит разные системные компоненты, в том числе память, связанную с центральным процессором 21. Системная шина 23 реализована, как любая известная из уровня техники шинная структура, содержащая в свою очередь память шины или контроллер памяти шины, периферийную шину и локальную шину, которая способна взаимодействовать с любой другой шинной архитектурой. Системная память содержит постоянное запоминающее устройство (ПЗУ) 24, память с произвольным доступом (ОЗУ) 25. Основная система ввода/вывода (BIOS) 26, содержит основные процедуры, которые обеспечивают передачу информации между элементами персонального компьютера 20, например, в момент загрузки операционной системы с использованием ПЗУ 24.

Персональный компьютер 20 в свою очередь содержит жесткий диск 27 для чтения и записи данных, привод магнитных дисков 28 для чтения и записи на сменные магнитные диски 29 и оптический привод 30 для чтения и записи на сменные оптические диски 31, такие как CD-ROM, DVD-ROM и иные оптические носители информации. Жесткий диск 27, привод магнитных дисков 28, оптический привод 30 соединены с системной шиной 23 через интерфейс жесткого диска 32, интерфейс магнитных дисков 33 и интерфейс оптического привода 34 соответственно. Приводы и соответствующие компьютерные носители информации представляют собой энергонезависимые средства хранения компьютерных инструкций, структур данных, программных модулей и прочих данных персонального компьютера 20.

Настоящее описание раскрывает реализацию системы, которая использует жесткий диск 27, сменный магнитный диск 29 и сменный оптический диск 31, но следует понимать, что возможно применение иных типов компьютерных носителей информации 56, которые способны хранить данные в доступной для чтения компьютером форме (твердотельные накопители, флеш карты памяти, цифровые диски, память с произвольным доступом (ОЗУ) и т.п.), которые подключены к системной шине 23 через контроллер 55.

Компьютер 20 имеет файловую систему 36, где хранится записанная операционная система 35, а также дополнительные программные приложения 37, другие программные модули 38 и данные программ 39. Пользователь имеет возможность вводить команды и информацию в персональный компьютер 20 посредством устройств ввода (клавиатуры 40, манипулятора «мышь» 42). Могут использоваться другие устройства ввода (не

отображены): микрофон, джойстик, игровая консоль, сканнер и т.п. Подобные устройства ввода по своему обычаю подключают к компьютерной системе 20 через последовательный порт 46, который в свою очередь подсоединен к системной шине, но могут быть подключены иным способом, например, при помощи параллельного порта, игрового порта или универсальной последовательной шины (USB). Монитор 47 или иной тип устройства отображения также подсоединен к системной шине 23 через интерфейс, такой как видеоадаптер 48. В дополнение к монитору 47, персональный компьютер может быть оснащен другими периферийными устройствами вывода (не отображены), например, колонками, принтером и т.п.

Персональный компьютер 20 способен работать в сетевом окружении, при этом используется сетевое соединение с другим или несколькими удаленными компьютерами 49. Удаленный компьютер (или компьютеры) 49 являются такими же персональными компьютерами или серверами, которые имеют большинство или все упомянутые элементы, отмеченные ранее при описании существа персонального компьютера 20, представленного на Фиг. 5. В вычислительной сети могут присутствовать также и другие устройства, например, маршрутизаторы, сетевые станции, пиринговые устройства или иные сетевые узлы.

Сетевые соединения могут образовывать локальную вычислительную сеть (LAN) 50 и глобальную вычислительную сеть (WAN). Такие сети применяются в корпоративных компьютерных сетях, внутренних сетях компаний и, как правило, имеют доступ к сети Интернет. В LAN- или WAN-сетях персональный компьютер 20 подключен к локальной сети 50 через сетевой адаптер или сетевой интерфейс 51. При использовании сетей персональный компьютер 20 может использовать модем 54 или иные средства обеспечения связи с глобальной вычислительной сетью, такой как Интернет. Модем 54, который является внутренним или внешним устройством, подключен к системной шине 23 посредством последовательного порта 46. Следует уточнить, что сетевые соединения являются лишь примерными и не обязаны отображать точную конфигурацию сети, т.е. в действительности существуют иные способы установления соединения техническими средствами связи одного компьютера с другим.

В заключение следует отметить, что приведенные в описании сведения являются примерами, которые не ограничивают объем настоящего изобретения, определенного формулой.

(57) Формула изобретения

1. Способ установки приложения, безопасный для устройств автоматизированной системы, согласно которому:

• получают конфигурацию безопасности для приложения, которое предназначено для установки на вычислительное устройство автоматизированной системы;

при этом конфигурация безопасности - это набор требований, предъявляемых к приложениям, выполнение которых обеспечивает требуемый уровень информационной безопасности автоматизированной системы;

• анализируют компоненты сборки приложения, предназначенного для установки на вычислительном устройстве автоматизированной системы, с целью проверки соответствия конфигурации безопасности;

• производят сборку приложения с использованием компонентов сборки, которые соответствуют конфигурации безопасности, в результате которой получают доверенный пакет приложения, при этом компонентом сборки является по меньшей мере файл исходного кода, а процесс сборки является компиляцией по меньшей мере одного файла

исходного кода;

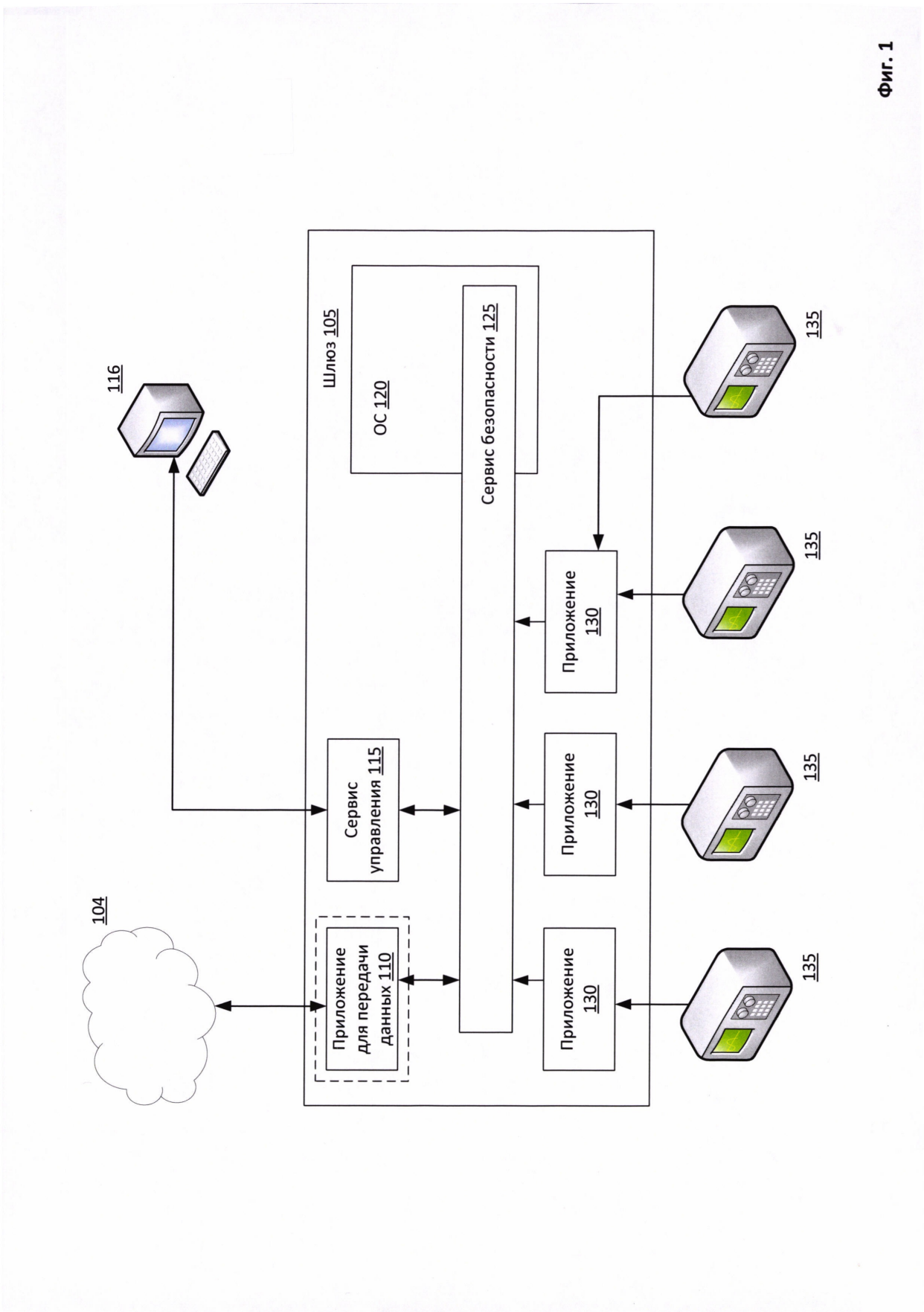
• производят установку приложения из доверенного пакета приложения на вычислительное устройство автоматизированной системы.

2. Способ по п. 1, в котором вычислительным устройством автоматизированной системы является устройство, имеющее доступ как к ресурсам за пределами сети автоматизированной системы, так и устройствам самой автоматизированной системы.

3. Способ по п. 1, в котором на этапе анализа компонентов сборки собирается информация об известных уязвимостях компонентов, а также используемых структурах данных и вызываемых методах.

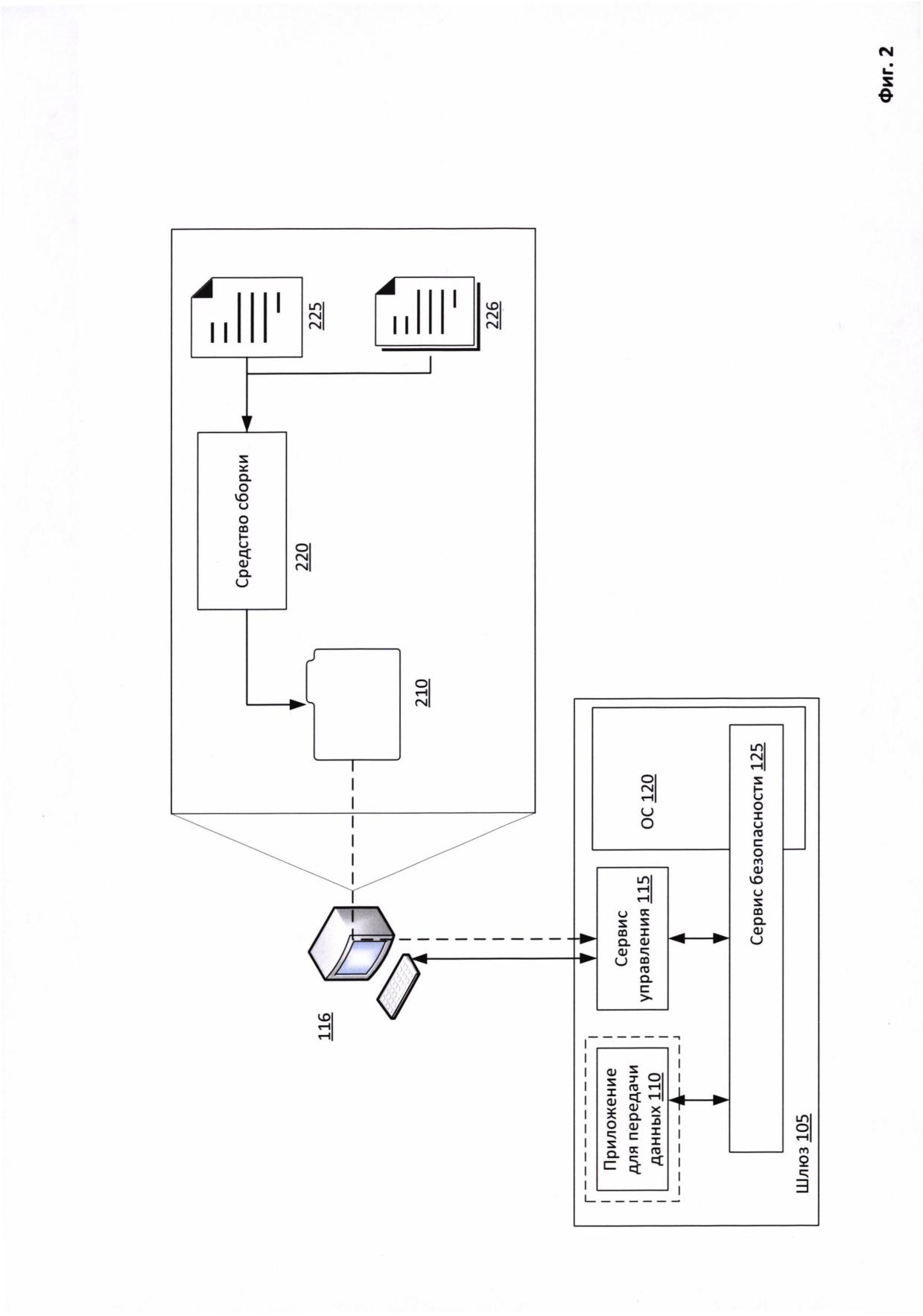
4. Способ по п. 1, в котором на этапе анализа компонентов сборки компоненты сборки, не соответствующие конфигурации безопасности, изменяются с целью соответствия упомянутой конфигурации безопасности.

1


116
Шлюз 105
ОС 120
Сервис безопасности 125
135
135
135
135
Приложение 130
Приложение 130
Приложение 130
Сервис управления 115
104
Приложение для передачи данных 110

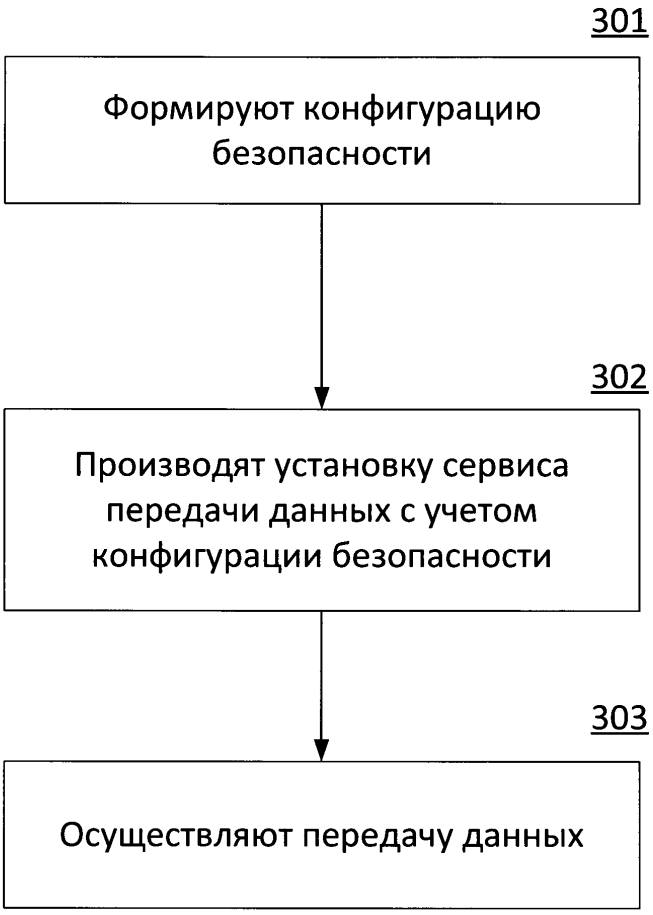
Фиг. 1

2


225
226
Средство сборки
220
210
116
Сервис управления 115
ОС 120
Сервис безопасности 125
Приложение для передачи данных 110
Шлюз 105

Фиг. 2

3

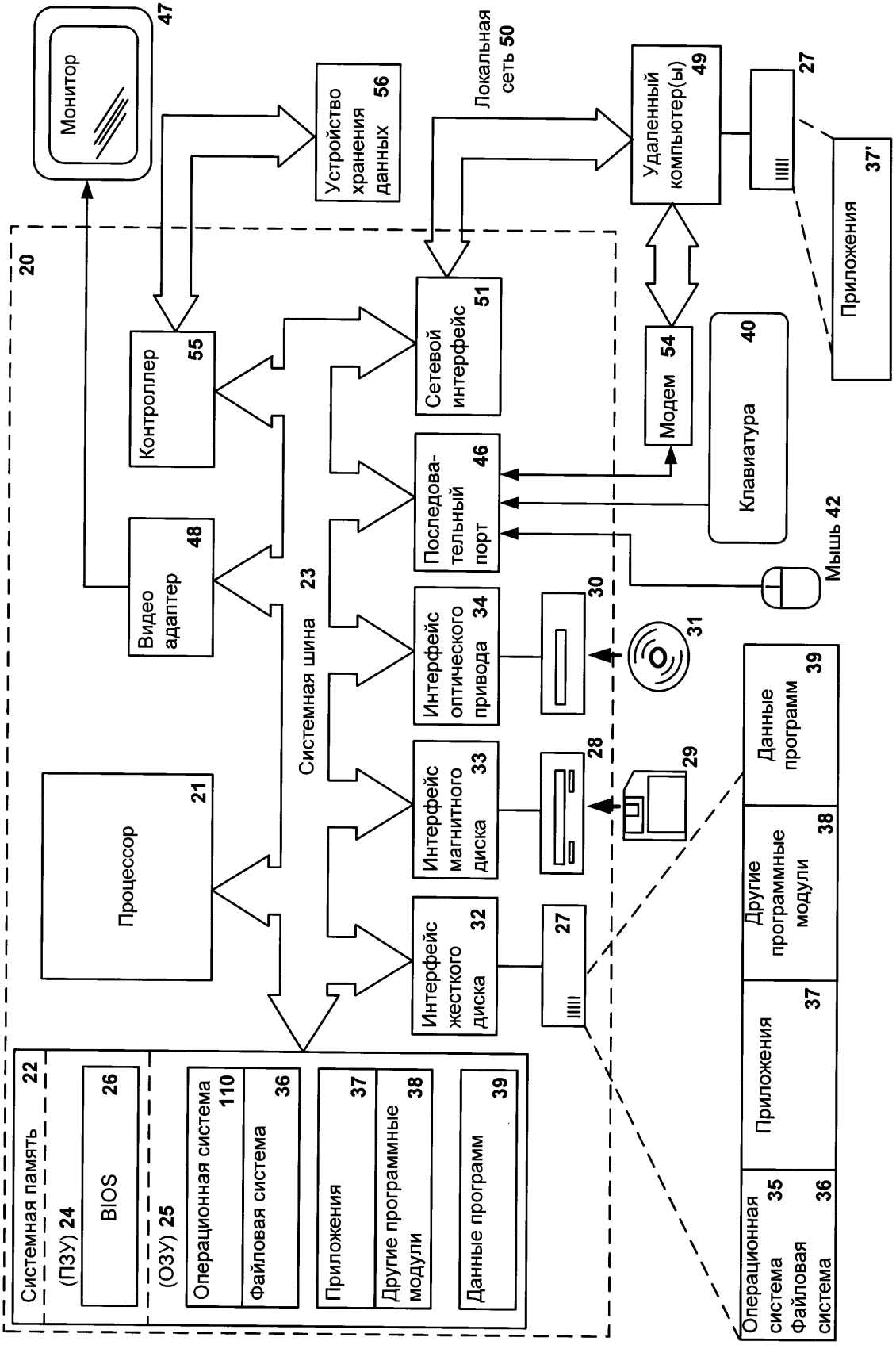

301
Формируют конфигурацию безопасности
302
Производят установку сервиса передачи данных с учетом конфигурации безопасности
303
Осуществляют передачу данных

Фиг. 3

4


401
Получают конфигурацию безопасности
402
Анализируют компоненты сборки сервиса
403
Производят сборку сервиса и использованием компонентов сборки, соответствующих конфигурации безопасности
404
Производят установку доверенного пакета сервиса

Фиг. 4


Монитор 47
Устройство хранения данных 56
Локальная сеть 50
Удаленный компьютер(ы) 49
27
Приложения 37'
20
Контроллер 55
Сетевой интерфейс 51
Модем 54
Клавиатура 40
Видео адаптер 48
Последова-тельный порт 46
Мышь 42
Системная шина 23
Интерфейс оптического привода 34
30
31
Процессор 21
Интерфейс магнитного диска 33
28
29
Данные программ 39
Другие программные модули 38
Интерфейс жесткого диска 32
27
Приложения 37
Операционная система 35
Файловая система 36
Системная память 22
(ПЗУ) 24
BIOS 26
(ОЗУ) 25
Операционная система 110
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39

Фиг. 5