РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 755 006**(13) **C2**

(51) МПК
G06F 21/53 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/53 (2021.02)

(21)(22) Заявка: **2020108171, 26.02.2020**

(24) Дата начала отсчета срока действия патента:
26.02.2020

Дата регистрации:
09.09.2021

Приоритет(ы):
(22) Дата подачи заявки: **26.02.2020**

(43) Дата публикации заявки: **26.08.2021** Бюл. № **24**

(45) Опубликовано: **09.09.2021** Бюл. № **25**

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

(72) Автор(ы):
Круглов Кирилл Николаевич (RU)

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

(56) Список документов, цитированных в отчете о поиске: **US 2016/0028768 A1, 28.01.2016. US 2015/0067862 A1, 05.03.2015. US 2015/0205966 A1, 23.07.2015. US 2016/0335110 A1, 17.11.2016. RU 2530210 C2, 10.10.2014.**

(54) Испытательный стенд мониторинга, контроля и анализа для оценки влияния вредоносного ПО на функционирование определенной конфигурации системы промышленной автоматизации и способ, реализующийся на нем

(57) Реферат:

Изобретение относится к области вычислительной техники. Технический результат заключается в повышении достоверности оценки влияния вредоносного ПО на функционирование определенной конфигурации системы промышленной автоматизации (СПА). Технический результат достигается за счет формирования на испытательном стенде определенной конфигурации инфраструктуры СПА согласно полученной спецификации, которая включает состав и задачи компонентов СПА; получения набора образцов вредоносного ПО; выполнения тестирования полученного набора на сформированном испытательном стенде, во время которого производят выявление причин и событий, приводящих к нарушению функционирования компонентов СПА и полевых элементов, за которые отвечает компоненты СПА, при этом тестирование включает определенный сценарии работы компонентов СПА, где во время указанного тестирования выявление причин и событий проводится на основании снимаемых параметров метрик, актуальных для тестируемой конфигурации СПА; произведения анализа выявленных причин и событий, приводящих к нарушению функционирования компонентов СПА на испытательном стенде на основании произведенных замеров параметров метрик, которые позволяют оценить производительность и временные сбои в работе компонентов СПА; определения влияния вредоносного ПО на конфигурацию СПА. 2 н. и 12 з.п. ф-лы, 7 ил.

RU 2755006 C2

RU 2755006 C2

Фиг. 2

RU 2755006 C2

RU 2755006 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 755 006**(13) **C2**

(51) Int. Cl.
G06F 21/53 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/53 (2021.02)

(21)(22) Application: **2020108171, 26.02.2020**

(24) Effective date for property rights:
26.02.2020

Registration date:
09.09.2021

Priority:
(22) Date of filing: **26.02.2020**

(43) Application published: **26.08.2021** Bull. № **24**

(45) Date of publication: **09.09.2021** Bull. № **25**

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

(72) Inventor(s):
Kruglov Kirill Nikolaevich (RU)

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

RU 2755006 C2

(54) TEST STAND FOR MONITORING, CONTROL AND ANALYSIS TO ASSESS THE IMPACT OF MALWARE ON THE FUNCTIONING OF A CERTAIN CONFIGURATION OF AN INDUSTRIAL AUTOMATION SYSTEM AND METHOD IMPLEMENTED ON IT

(57) Abstract:

FIELD: computer technology.

SUBSTANCE: certain configuration of the infrastructure of an industrial automation system (hereinafter – IAS) is formed on a test stand according to the obtained specification, which includes the composition and tasks of IAS components; a set of malware samples is obtained; the obtained set is tested on the formed test stand, during which causes and events leading to the malfunction of IAS components and field elements, for which IAS components are responsible, are identified, while testing includes a certain operation scenario of IAS components, where during the specified testing, the identification of causes and events is carried out based on removed parameters of metrics relevant to IAS configuration under test; identified causes and events leading to the malfunction of IAS components are analyzed on the test stand based on measurements of parameters of metrics that allow one to assess the performance and temporary failures in IAS components; the impact of malware on IAS configuration is determined.

EFFECT: technical result is an increase in the reliability of assessing the impact of malware on the functioning of a certain configuration of IAS.

14 cl, 7 dwg

RU 2755006 C2

Фиг. 2

RU 2755006 C2

RU 2755006 C2

Область техники

Настоящее изобретение относится к испытательной и информационно-измерительной технике, предназначенной для мониторинга, анализа и контроля при оценке влияния образцов исследуемого ПО, в частности вредоносного ПО, на функционирование определенной конфигурации системы промышленной автоматизации.

Уровень техники

В настоящее время наблюдается интерес к объектам критической инфраструктуры со стороны различных злоумышленников. Объектами критической инфраструктуры являются объекты в таких промышленных областях как электроэнергетика, водоснабжение, нефтегазовая промышленность и автомобилестроение, а также системы автоматизации зданий и объекты хранения и передачи данных. Данные объекты содержат различные системы промышленной автоматизации, например, системы промышленного контроля (англ. Industrial Control System или ICS). В свою очередь одним из примеров системы промышленного контроля является автоматизированная система управления технологическими процессами (АСУ ТП).

Обеспечение безопасности АСУ ТП является специфическим процессом, имеющим ряд отличий от традиционной борьбы с киберугрозами. Киберугроза - это совокупность факторов и условий, создающих опасность нарушения информационной безопасности. В частности, стратегия защиты в основном нацелена на сохранение работоспособности технологического процесса, в отличие от корпоративных систем, в которых важнее сохранить конфиденциальность и доступность данных.

Большое количество угроз промышленным системам и их АСУ ТП связано с обычным вредоносным ПО, т.е. не предназначенным для целевых кибератак. Под обычным вредоносным ПО подразумевается такое вредоносное ПО, которое не разрабатывалось специально для атаки на промышленные системы. Тем не менее, как показал опыт, даже если их влияние на работу IT-систем незначительно, то они могут влиять на целостность и доступность компонентов АСУ, и как одно из следствий косвенно влиять на стабильность технологического и производственного процессов.

Например, такие вредоносные программы как шифровальщики (англ. encryption malware) и программы, целью которых является уничтожение файлов с жесткого диска компьютера (англ. wiper), оказывают разрушительное техническое воздействие на автоматизированные системы управления (АСУ) и ИТ - системы различных технологических систем.

Майнеры, которые относительно безвредные в офисной сети, в процессе своей работы и распространения могут привести к отказу в обслуживании некоторых компонентов АСУ ТП. Майнер - программа для добычи крипто-валюты за счет использования значительных вычислительных ресурсов.

Сетевые черви (разновидность вредоносной программы) представляют большую опасность как для IT-систем, так и для технологических сетей, в которых последствия их действий могут быть гораздо более значительными. Например, найденные на многих компьютерах АСУ сетевые черви самостоятельно распространялись через сетевые папки и съемные носители, уничтожая при этом данные на зараженных устройствах, а также по локальной (LAN) и глобальной сетям (WAN) при помощи эксплойтов. В ряде случаев такие действия способны не только вызвать отказ в обслуживании АСУ и, в частности, систем мониторинга и телеуправления, но и привести к аварийным ситуациям.

Многофункциональные программы-шпионы, как правило, способны не только похищать конфиденциальную информацию, загружать и выполнять другое вредоносное

ПО, но и предоставлять злоумышленникам возможность несанкционированного удаленного управления зараженными устройствами. Такие программы еще называют бэкдорами (от англ. backdoor).

Последствия от активностей на компьютерах указанными вредоносными программами зависят от важности атакуемых технологических систем для производственного процесса и бизнес-процессов предприятия. Во многих случаях несоразмерно сильное воздействие указанных вредоносных программ происходит на АСУ. Этот эффект в первую очередь связан со спецификой архитектуры и внедрением в системы АСУ. В итоге, вредоносное ПО, не оказывающее существенного негативного влияния на ИТ-системы предприятия, может привести к простоям систем в промышленной сети и нарушению производственных процессов.

Также стоит отметить, что не только вредоносное ПО может оказать существенное негативное влияние на системы промышленного контроля (СПК), в частности на автоматизированные системы управления, но и легальное ПО, которое содержит ошибки, способные привести к нерассчитанному поведению и нарушению работы СПК.

Кроме того, безопасность промышленных систем от внешних компьютерных угроз является сама по себе актуальной задачей. В частности, необходимо управлять и обеспечивать безопасность промышленных контроллеров (англ. Programmable Logic Controller) и автоматизированных систем управления.

В то же время, чтобы создать необходимый уровень защиты от угроз, необходимо произвести предварительную оценку рисков промышленных систем, которая позволяла бы учитывать внешние воздействия на различные элементы (например, PLC, SCADA, SiS) промышленных систем на основании обычного ПО и/или вредоносного ПО. Примером угрозы являются атаки на элементы промышленных систем, при этом указанные элементы информируют об отказе в обслуживании. Обычная стратегия заключается в тестировании каждого отдельного устройства ICS в каждой конфигурации. Это часто вызывает проблемы, потому что обычная стратегия требует приобретения и размещения устройств ICS, что может оказаться дорогостоящим делом. Кроме того, как себя поведет тот или иной элемент в промышленной сети, которая в большинстве случаев будет уникальной на конкретном промышленном объекте, также не известно.

Таким образом, существует потребность в таких решениях, которые позволят предварительно определить условия возникновения отказов в обслуживании промышленных систем и их элементов (компонентов) АСУ, вызванных косвенными действиями указанного вредоносного ПО. Настоящее изобретение позволяет произвести оценку влияния программного обеспечения, в частности вредоносного ПО, на доступность (работоспособность) систем промышленной автоматизации, в частности автоматических систем управления.

Раскрытие изобретения

Настоящее изобретение было выполнено с учетом описанных выше проблем и недостатков известного уровня техники, и цель настоящего изобретения состоит в том, чтобы выявить слабые стороны различных систем промышленной автоматизации таких как систем промышленного контроля (англ. Industrial Control System или ICS) на основании оценки влияния различного ПО, в частности вредоносного ПО, на работоспособность или доступность систем промышленного контроля, в частности АСУ ТП.

Настоящее изобретение позволяет по крайней мере произвести оценку влияния вредоносного ПО на функционирование определенной конфигурации системы промышленной автоматизации (СПА). В зависимости от вариантов исполнения

настоящего изобретения (систем и способов) производится в процессе указанной оценки по крайней мере одно из следующих действий:

• проведение анализа вредоносного ПО в имитируемой среде типа «песочница» (англ. sandbox) с последующим выявлением подходящего вредоносного ПО для тестирования определенной конфигурации СПА, в частности АСУ ТП,

• выполнение контролируемого тестирования образцов вредоносного ПО в имитируемой среде определенной конфигурации СПА, в частности АСУ ТП,

• выявление и измерение влияние каждого образца вредоносного ПО для определенной конфигурации СПА, в частности АСУ ТП,

• проведение анализа всех выявленных причин (событий), приводящих к нарушению функционирования определенной конфигурации СПА,

• вынесение решения об опасности определенного образца вредоносного ПО к определенной конфигурации СПА.

Варианты реализации настоящего изобретения включают в себя также возможность формирования соответствующего отчета, содержащего признаки компрометации, полученные в результате вредоносной деятельности по крайней мере одного образца вредоносного ПО, где в качестве компрометирующих признаков указываются по крайней мере причины или события, повлиявшие на то или иное нарушение в функционирование СПА. Кроме того, настоящее изобретение также позволяет произвести оценку влияния легитимного ПО на функционирование определенной конфигурации СПА.

Первый технический результат настоящего изобретения заключается в расширении арсенала технических средств для оценки влияния исследуемого ПО на работоспособность определенной конфигурации систем промышленной автоматизации.

Второй технический результат настоящего изобретения заключается в повышении достоверности оценки влияния вредоносного ПО на функционирование определенной конфигурации системы промышленной автоматизации.

В качестве одного варианта исполнения настоящего изобретения предлагается испытательный стенд мониторинга, контроля и анализа для оценки влияния образцов вредоносного ПО на функционирование определенной конфигурации системы промышленной автоматизации (СПА), при этом испытательный стенд включает изменяемый набор различных компонентов СПА, средство мониторинга доступности и средство оценки влияния, при этом указанный стенд получает спецификацию определенной конфигурации СПА и, по крайней мере, один образец вредоносного ПО.

Другой вариант исполнения испытательного стенда дополнительно включает средство отбора вредоносного ПО.

В еще одном варианте исполнения испытательного стенда средство отбора вредоносного ПО производит отбор образов вредоносного ПО на основании исследования исполнения различного ПО в изолированной среде с последующим анализом сформированного журнала активностей по итогам исследования для выявления воздействий, представляющих потенциальную угрозу функциональности СПА.

Другой вариант исполнения испытательного стенда имеет доступ в информационно-коммуникационную сеть для удаленного взаимодействия.

В еще одном варианте исполнения испытательного стенда нарушением функционирования испытательного стенда, имитирующего определенную конфигурацию СПА, является по крайней мере выявление события, указывающего на отказ в обслуживание по крайней мере одного компонента СПА.

Другой вариант исполнения испытательного стенда средство оценки влияния дополнительно производит формирование рекомендаций.

В еще одном варианте исполнения испытательного стенда рекомендации содержат по крайней мере одно из следующих сведений:

• позволяющие обнаруживать признаки заражения СПА вредоносным ПО, в том числе без установки антивирусного ПО;

• по защите от заражения от вредоносного ПО;

• об устранении заражения и его последствий;

• о корректировке компонента СПА или сетевого трафика, которые подвержены влиянию вредоносного ПО;

• о проведении дополнительных исследований.

В качестве другого варианта исполнения настоящего изобретения предлагается способ оценки влияния вредоносного ПО на работоспособность системы промышленной автоматизации (СПА), реализующийся при помощи испытательного стенда по п. 1, заключающийся в том, что формирует на испытательном стенде определенную конфигурацию инфраструктуры СПА согласно полученной спецификации, которая включает состав и задачи компонентов СПА; получает набор образцов вредоносного ПО; выполняет тестирование полученного набора на сформированном испытательном стенде, во время которого производит выявление причин, приводящих к нарушению функционирования компонентов СПА и полевых элементов, за которые отвечает компоненты СПА, при этом тестирование включает определенный сценарии работы компонентов СПА; производит анализ выявленных причин, приводящих к нарушению функционирования компонентов СПА на испытательном стенде; определяет влияние вредоносного ПО на СПА.

В другом варианте исполнения способа инфраструктура СПА представляет собой как сетевое оборудование и компьютер пользователя (оператора), так различные компоненты автоматизированных систем управления (АСУ).

В еще одном варианте исполнения способа компонентами АСУ по крайней мере являются системы диспетчерского управления и сбора данных, распределенные системы управления, системы противоаварийной защиты, системы на программируемых логических контроллерах и шлюзы данных.

В другом варианте исполнения способа формируют испытательный стенд путем виртуализации.

В еще одном варианте исполнения способа формируют испытательный стенд путем включения в единую сеть только тех компонентов, которые входят в состав конфигурации инфраструктуры СПА согласно спецификации.

В другом варианте исполнения способа дополнительно получаемый набор образцов вредоносного ПО, был сформирован на основании анализа вредоносного ПО в имитируемой среде типа «песочница» с последующим выявлением подходящего вредоносного ПО для тестирования определенной конфигурации инфраструктуры СПА.

В еще одном варианте исполнения способа дополнительно на шаге д) определяют степень влияния вредоносного ПО на СПА, где степень указывает на критичность вредоносного ПО в отношении к конфигурации СПА.

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:

На Фиг. 1 представлен пример промышленной инфраструктуры, для которой реализуется заявленное изобретение.

На Фиг. 2 схематично представлена система оценки влияния исследуемого ПО, которое вызывает отказ в обслуживание компонентов систем промышленной автоматизации, с возможностью реализовать различные варианты осуществления.

На Фиг. 3 схематично представлен пример исполнения испытательного стенда, имитирующего определенную конфигурацию СПА.

На Фиг. 4 схематично представлен пример сценария влияния вредоносного ПО на АСУ, при котором происходит отказ в обслуживании.

На Фиг. 5 представлена блок-схема, иллюстрирующая способ оценки влияния исследуемого ПО на компоненты систем промышленной автоматизации.

На Фиг. 6 представлена блок-схема, иллюстрирующая частный случай реализации представленного способа на Фиг. 5, а именно, способа оценки влияния вредоносного ПО, которое вызывает отказ в обслуживании компонентов определенной конфигурации СПА.

Фиг. 7 иллюстрирует пример компьютерной системы общего назначения, с помощью которого может быть реализовано заявленное изобретение.

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. Приведенное описание предназначено для помощи специалисту в области техники для исчерпывающего понимания изобретения, которое определяется только в объеме приложенной формулы.

Настоящее изобретение позволяет по крайней мере произвести оценку влияния исследуемого ПО на функционирование (работоспособность) определенной конфигурации инфраструктуры системы промышленной автоматизации (СПА). В первую очередь под СПА подразумевается различные системы промышленного контроля (СПК), объединенные промышленной информационно-коммуникационной сетью. В свою очередь примером СПК является автоматизированная система управления технологическими процессами (АСУ ТП) и ее компоненты. АСУ ТП -группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях. Примерами компонентов АСУ ТП являются: системы диспетчерского управления и сбора данных (от англ. Supervisory Control And Data Acquisition, SCADA), распределенные системы управления (англ. Distributed Control System, DCS), системы противоаварийной защиты (англ. Safety instrumented Systems, SiS), системы на программируемых логических контроллерах (англ. Programmable Logic Controller, PLC), шлюзы данных (англ. OPC), сетевое оборудование, объединяющее указанные системы в технологическую сеть, и т.п.

В рамках заявленного изобретения под исследуемым ПО в первую очередь

понимается вредоносным ПО, но не ограничивается им. Также в качестве исследуемого ПО может быть использовано ПО, которое способно нанести ущерб функционированию СПА. Примерами такого исследуемого ПО являются:

• легальное ПО, несовместимое или частично совместимое с СПА или ее компонентами,

• легальное ПО, содержащее ошибки, способные привести к нерасчетному поведению СПА или ее компонентов,

• специализированное (сертифицированное) ПО, которое было модернизировано или выпущена новая версия,

• несертифицированное ПО, которое, как правило, является легальным и при этом предназначено непосредственно для работы компонента СПА,

• недоверенное ПО, под которым подразумевается ПО, действия которого могут вызвать отказ в обслуживании компонента СПА или привести к аварийным ситуациям.

Таким образом, заявленное изобретение позволяет обнаруживать любые аномалии в работе исследуемого ПО и производить оценку влияния указанного исследуемого ПО на совместимость или несовместимость с целевым ПО в промышленных системах и сетях. Также стоит сказать, что среди вредоносного ПО есть нецелевое вредоносное ПО. Нецелевым вредоносным ПО называют такое вредоносное ПО, которое изначально не было создано для причинения какого-либо ущерба непосредственно промышленным системам и сетям. Скорее всего, влияние и наносимый ущерб нецелевым вредоносным ПО являются побочным эффектом или даже результатом ошибки разработчика такого ПО.

Для оценки влияния исследуемого ПО на работоспособность, например, АСУ ТП и подобных систем представленное изобретение имеет следующие функциональные возможности:

1) Автоматизированный анализ функциональности и поведения компьютерных программ, обнаруженных как на персональных компьютерах пользователей, так и в сети, с последующим выявлением типов и самих образцов исследуемого ПО, которые потенциально способны нанести ущерб системам АСУ ТП.

2) Проведение по крайней мере одного автоматизированного исследования на испытательном стенде, имитирующем определенную конфигурацию АСУ ТП или же нескольких различных АСУ, для по крайней мере одного исследуемого ПО в ходе отбора, представленного в пункте 1. В ходе исследования оценивается воздействие ПО, которое функционирует в представленной конфигурации АСУ ТП на испытательном стенде, по различным параметрам, включающим такие параметры как производительность и временные сбои в работе АСУ и ее компонентов или объектов, которые управляются АСУ.

3) Классификацию исследуемого ПО (в частности, вредоносного ПО) согласно его влиянию на АСУ ТП и определения признаков компрометации и артефактов, полученных в результате анализа влияния исследуемого ПО на АСУ ТП, с последующим созданием образцов (сигнатур) или правил поведения, позволяющих обнаружить признаки нахождения или заражения АСУ ТП соответствующим ПО.

4) Дополнительно принимать решения о проведении дополнительных исследований или возможных мерах по защите от исследуемого (вредоносного) ПО как непосредственно в системе АСУ ТП, так и в информационно-коммуникационной сети, с помощью которой АСУ связана с другими устройствами или системами промышленного объекта.

В качестве одних из преимуществ настоящего изобретения перед предшествующим

уровнем техники выделяются такие возможности как:

• выявление и последующая классификация ПО, в том числе и вредоносного ПО, оказывающего существенное влияние на определенную конфигурацию АСУ ТП;

• выявление слабых сторон определенных конфигураций АСУ ТП с последующим формированием соответствующей отчетности;

• формирование испытательного стенда, имитирующего определенную конфигурацию инфраструктуры АСУ ТП или всей СПА с последующим тестированием образцов исследуемого ПО на указанном стенде.

На Фиг. 1 представлен пример архитектуры промышленной инфраструктуры 100, для которой реализуется заявленное изобретение. Промышленная инфраструктура 100 может имеет пять различных сетевых уровней взаимодействия. Первым сетевым уровнем является полевой уровень, который включает в себя ряд используемых промышленных (полевых) устройств. Примерами полевых устройств являются датчики, клапаны, преобразователи, исполнительные механизмы, такие как насос, лазер или токарный станок, а также другие устройства. Вторым сетевым уровнем является технологическая сеть, которая включает различные промышленные контроллеры, в частности программируемый логический контроллеры (ПЛК/PLC). Контроллеры производят управления полевыми устройствами и взаимодействуют с компонентами третьего сетевого уровня. Третьим сетевым уровнем является уровень управления (распределенная вычислительная сеть), который включает в себя рабочие станции (компьютеры), сервера и сетевые устройства. Рабочая станция может содержать автоматизированную систему управления технологическим процессом (АСУ ТП), например, SCADA. Сервера могут выполнять функции вычисления, управления и контроля. Четвертым уровнем является уровень предприятия (офисная сеть), которая как правило включает в себя персональные рабочие станции сотрудников промышленного предприятия и сервера. Пятым сетевым уровнем является уровень взаимодействия с внешними, по отношению к предприятию, необходимыми устройствами, связь с которыми может производиться через информационно - коммуникационную сеть типа сеть Интернет.

Примеры систем промышленной автоматизации (СПА) могут включать в себя один или несколько промышленных контроллеров, которые облегчают мониторинг и управление соответствующими промышленными устройствами и процессами. Промышленные контроллеры, такие как ПЛК, могут обмениваться данными с полевыми устройствами с помощью встроенных проводных входов/выходов (I/O) и/или через заводскую сеть, объединяющую технологическую сеть и сеть уровня управления. Промышленный контроллер обычно может принимать любые комбинации цифровых или аналоговых сигналов от полевых устройств, которые могут показывать текущее состояние промышленных устройств и/или связанных с ними промышленных процессов (например, температура, положение, присутствие или отсутствие компонентов, уровень жидкости и т.д.), и может выполнять ранее определенную пользователем программу управления, которая может выполнять автоматизированное принятие решений для контролируемых промышленных процессов на основе полученных сигналов. Такие программы управления также называют целевым ПО. Промышленный контроллер может выдавать соответствующий цифровой и/или аналоговый управляющий сигнал на полевые устройства в соответствии с решениями, принятыми управляющей программой. Выходы могут содержать сигналы управления устройством, сигналы управления температурой или положением, рабочие команды роботу для обработки или перемещения материалов, сигналы управления микшером, сигналы управления

движением и т.д. Программа управления может содержать любой подходящий тип кода, который может быть использован для обработки входных сигналов, считанных в контроллер, и для управления выходными сигналами, генерируемыми промышленным контроллером, включая, помимо прочего, лестничную логику, функциональные диаграммы, блок-схемы функций, структурированный текст или другие подобные платформы.

На Фиг. 2 схематично представлена система оценки влияния исследуемого ПО на функционирование определенной конфигурации инфраструктуры СПА, в частности, на АСУ ТП 200. Конфигурации инфраструктуры СПА формируются на основании объединения определенных компонентов или устройств, из которых состоит архитектура промышленной инфраструктуры 100, представленной на Фиг. 1.

При проверке функционирования АСУ ТП в первую очередь производится проверка на такой признак работоспособности АСУ ТП как выявление отказа в обслуживании по крайней мере одного компонента АСУ ТП или самой АСУ ТП. Система оценки влияния исследуемого ПО на функционирование АСУ ТП (далее - система оценки) 200 функционально включает по меньшей мере испытательный стенд 210, средство отбора ПО 220, средство мониторинга доступности 230 и средство оценки влияния исследуемого ПО (далее - средство оценки влияния) 240. Представленный состав соответствует функциональному представлению системы оценки 200, при этом реализация средств может быть различной. Средства системы оценки 200 могут быть реализованы как совместно в одном устройстве, например, средства 220, 230 и 240 входят в состав испытательного стенда 210, так и каждое указанное средство может быть реализовано на отдельном компьютере, пример которого представлен на Фиг. 7, при это все компьютеры будет объединены в сеть, например, в технологическую сеть.

Испытательный стенд 210 предназначен для проведения тестирования полученной или сформированной согласно спецификации определенной конфигурации АСУ ТП с помощью полученного по крайней мере образца одного исследуемого ПО от средства отбора ПО 220. Во время тестирования между компонентами АСУ ТП производится обмен данными. Испытательный стенд 210 позволяет повторить определенные конфигурации АСУ ТП согласно имитации по крайней мере одной управляющей программы для проведения их тестирования. Создание испытательного стенда 210, имитирующего определенную конфигурацию АСУ ТП, может быть произведено как с помощью реальных компонентов АСУ ТП, так и при помощи виртуальных компонентов АСУ ТП. Реализация зависит от варианта реализации самого стенда 210. При использовании виртуальных компонентов соответственно стенд 210 будет также являться виртуальным и реализуется на вычислительном устройстве при помощи соответствующих технологий, так, например, при помощи виртуализации и симуляции.

При реализации стенда 210 при помощи аппаратного обеспечения (оборудования) подбор компонентов для имитации определенной конфигурации АСУ ТП осуществляется согласно полученной спецификации состава АСУ ТП и функциональных возможностей компонентов. В зависимости от функциональных возможностей производится соответствующий им информационный обмен данными между компонентами во время тестирования. Например, конфигурация АСУ ТП представляет собой технологическую сеть, объединяющую по крайней мере один контроллер PLC и по крайней мере одну систему SCADA. Системы SCADA и контроллеры PLC размещены на различных компьютерах (оборудовании). При этом компьютер с системой SCADA (далее в примере - К1) производит обмен данными с каждым компьютером контроллеров PLC (далее в примере - К2). Так, К1 каждую секунду запрашивает у К2 информацию о состоянии и

режиме работы оборудования, которое контролирует соответствующий контроллер PLC.

Предварительная подготовка стенда 210, а именно, формирование определенной конфигурации АСУ ТП для оценки осуществляется либо при помощи оператора (пользователя) испытательного стенда 210, либо автоматически. При автоматическом варианте реализации стенд 210 уже представляется собой технологическую сеть, объединяющую большую совокупность различных компонентов АСУ ТП, которые объединены по крайней мере в одну общую информационно-коммуникационную сеть (далее - сеть). При получении спецификации состава АСУ ТП производится включение или отключение тех или иных компонентов на испытательном стенде 210 до тех пор, пока не будет сформирована определенная конфигурация АСУ ТП согласно спецификации. Стоит отметить, что формирование определенной конфигурации АСУ на стенде 210 как правило основывается на повторении настоящей технологической сети, для проведения испытания.

Другими словами, испытательный стенд позволяет производить мониторинг, контроль и анализ для определения влияния образцов исследуемого и, в частности вредоносного, ПО на функционирование определенной конфигурации СПА с помощью по меньшей мере средства мониторинга доступности 230 и средства оценки влияния 240, при этом указанный стенд получает спецификацию определенной конфигурации СПА и, по крайней мере, образец одного исследуемого ПО от средства отбора ПО 220.

Средство отбора ПО 220 предназначено для формирования набора образцов исследуемого ПО для передачи его испытательному стенду 210 и/или средству мониторинга доступности 230, при этом указанный набор по меньшей мере содержит образец одного исследуемого ПО. Отбор образцов ПО для указанного набора осуществляется на основании контролируемого исследования исполнения исследуемого ПО с последующим формированием журнала событий и его анализа для выявления воздействий, представляющих угрозу доступности или работоспособности, а также целостности конфигурации АСУ ТП. Доступность подразумевает наличие доступа к конфигурации АСУ ТП или ее компонентам, т.е. в отсутствии отказа в обслуживание.

Формирование указанного набора, например, производится следующим образом. Средство отбора 220 получает образцы вредоносного ПО из внешней сети. Внешней сетью является сеть Интернет. Стоит отметить, что вредоносного ПО огромное количество. Поэтому средство отбора 220 в зависимости от варианта реализации может получать как наиболее популярные образцы вредоносного ПО, так и представляющие наибольшую угрозу. Наибольшая угроза характеризуется высоким риском нанести ущерб. Еще одним ограничивающим критерием при выборе образцов вредоносного ПО может являться - получение наиболее популярного вредоносного ПО для определенного вида устройств или оборудования, а также для определенной конфигурации СПА. Устройства используют различные платформы при функционировании, например, x86 и ARM. Полученные образцы вредоносного ПО исследуются при помощи технологии «песочница» (от англ. Sandbox). Под технологией «песочница» понимается специально выделенная (изолированная) среда на компьютере для безопасного исполнения компьютерных программ. Примером такой среды является виртуальная машина. Песочница реализуется в рамках средства отбора 220, которое в свою очередь может быть реализовано при помощи компьютера, представленного на Фиг. 7. В зависимости от варианта реализации «песочница» может представлять собой как стандартную среду, например, имитирующую персональный компьютер, так и специфичную среду, где спецификой среды является наличие компонента SCADA

и/или запущенные в указанной среде процессы, файлы на диске, ключи реестра и сетевые порты, которые специфичны для технологических сетей.

Во время анализа формируется для каждого вредоносного ПО журнал событий, содержащий все активности, произошедшие во время исполнения вредоносного ПО в изолированной среде. На основании анализа журнала активностей каждого вредоносного ПО средство отбора 220 производит отбор вредоносного ПО, подходящего для тестирования на испытательном стенде 210. Так, отбор образцов осуществляется на основании ряда признаков, которые характеризуют/указывают, как говорилось выше, на воздействия, представляющие угрозу доступности или работоспособности, а также целостности определенной конфигурации АСУ ТП. Примерами таких признаков по крайней мере являются следующие:

• производится манипуляция с памятью других процессов, где манипуляцией является операторы чтения или записи;

• производится выделение большого объема памяти, например, больше или равно 1Гб;

• совершается множество операций с файлами (чтение/запись файлов), где под множеством операций может подразумеваться от двух и более операции и зависит от конкретного файла;

• совершается манипуляция с системными настройками, например, в конфигурационных файлах и/или реестре;

• совершается манипуляция с системными файлами, например, осуществляется запись в них;

• совершается множество операций с реестром, связанных с записью в него, где под множеством операций может подразумеваться от двух и более операции;

• производится загрузка драйвера;

• производятся манипуляции над запущенными процессами в песочнице, специфичные для технологических сетей.

При выявлении по крайней мере одного из критериев отбора во время анализа журнала событий средство отбора ПО 220 принимает решение о соответствии образца вредоносного ПО для проведения последующего тестирования на испытательном стенде 210, имитирующем определенную конфигурацию АСУ ТП. В этом случае образец вредоносного ПО включается в указанный набор образцов исследуемого ПО для передачи его испытательному стенду 210. Такой отбор исследуемого ПО позволяет в последствии более персонализировано подойти к тестированию определенных конфигураций СПА.

Средство мониторинга доступности 230 предназначено для контроля проводимого автоматизированного тестирования определенной конфигурации АСУ ТП, имитирующейся на испытательном стенде 110. Во время указанного тестирования средство 130 выявляет влияние каждого образца исследуемого ПО на доступ к каждому компоненту, содержащемуся в тестируемой АСУ ТП, или на определенную конфигурацию АСУ ТП в целом. Кроме того, в одном из вариантов реализации средство 230 так же обладает функционалом, который позволяет измерить уровень/степень выявленного влияния, где измерение может быть, как вероятностным, так и определенным, на основании предварительно сформированной шкалы.

В одном из вариантов реализации средство 230 может представлять из себя сервер или маршрутизатор, который производит информационный обмен определенными данными между компонентами АСУ ТП и снимает параметры метрик, актуальных для тестируемой АСУ ТП. При этом обмен данными производится с помощью «зеркального

порта» или зеркалирования, т.е. производится дублирование пакетов одного порта сетевого коммутатора на другой. Метрики определяются согласно конфигурации АСУ ТП. Полный перечень метрик, которые средство 130 может измерить/снять, хранятся в базе данных (не представлена на Фиг. 2).

В еще одном варианте реализации, тестирование на стенде 210 проводится средством мониторинга доступности 230. Для проведения тестирования средство 230 получает от средства отбора 220 набор образцов исследуемого ПО. Далее средство 230 формирует серию автоматизированных испытаний в зависимости от количества образцов исследуемого ПО в полученном наборе и компонентов, из которых состоит конфигурация АСУ ТП, имитируемая на стенде 210. Сформированная серия включает по крайней мере одно испытание. Сценарий каждого испытания описывает взаимодействие между компонентами тестируемой АСУ ТП и используемый по крайней мере образец одного исследуемого ПО. Тестирование заключается по крайней мере в одном проведении сценария взаимодействия компонентов тестируемой АСУ ТП после заражения/внедрения по крайней мере образца одного исследуемого ПО в технологическую сеть испытательного стенда 210.

Рассмотрим пример одного сценария испытания.

Предположим, что АСУ ТП включает два компонента:

• компьютера А, содержащий систему SCADA,

• компьютер Б, содержащий контроллер PLC, который в свою очередь производит контроль работы насоса.

Согласно сценарию, в стенд 210 был внедрен образец одного вредоносного ПО. Насос предназначен для заполнения бака водой. Компьютер А производит обмен данными с компьютером В согласно протоколу OPC UA. Так, компьютер А каждую секунду запрашивает у компьютера Б информацию о состоянии и режиме работы насоса, где данные о режиме работы содержат информацию: включен или выключен, сколько воды качает и сколько воды было прокачено насосом (залито в бак). В случае, когда бак наполнен компьютер А отправляет компьютеру В команду выключить/остановить насос.В данном примере метриками для оценки являются:

• скорость отправки запросов от компьютера А компьютеру Б,

• время задержки в реакции компьютера А на ситуацию, когда компьютер Б сообщает о наполненности бака.

В таком сценарии исследования, если образец вредоносного ПО окажет некое воздействие, которое увеличит время обработки запроса информации о состоянии и ответ на запрос информации будет отправляться не раз в одну секунду, а раз в 3 или более секунды, то возможна ситуация, когда компьютер А поздно среагирует на переполнение бака.

Еще одним примером сценария является ситуация, когда у компонента (например, упомянутого насоса) задан определенный разрешающий диапазон параметров. Время выключения насоса до 1 секунды, при этом в процессе эксплуатации было определено, что в среднем выключение происходит за 0.2 секунды. При испытании производится тестировании вредоносного ПО, которое приводит к тому, что среднее время выключения насоса стало уже 0.8 секунд. Что еще не критично, но при этом становится мало времени для непредвиденной ситуации. Так как просесть производительность насоса может и по легальным причинам, и на это не будет ресурса времени.

В ходе испытаний средство 230 формирует отчет о воздействии исследуемого ПО, который внедрен в стенд 210 (тестируемую АСУ ТП) по параметрам метрик, которые в первую очередь позволяют оценить производительность и временные сбои в работе

АСУ ТП (отказ в обслуживание).

Примером типичного сбоя в работе АСУ ТП является ситуация, когда сетевые службы или весь компьютер не выполняют функции, которые от них ожидают. В предыдущем примере, если компьютер А не будет опрашивать компьютер Б то, при работающем насосе бак переполнится, что может повлечь поломку как насоса, так и наступление более тяжелых последствий.

Результаты проведенных испытаний (например, в виде отчета) средство 230 передает средству оценки влияния 240. Результаты содержат информацию по крайней мере об одном из: работоспособности, производительности, эффективности и эксплуатационных качествах как АСУ ТП в целом, так и каждого его компонента, об обмене данными при взаимодействии компонентов, любых отклонения, произошедшие в АСУ ТП, и об образцах исследуемого ПО, которые были использованы в испытаниях.

Средство оценки влияния 240 предназначено для оценки степени влияния исследуемого ПО на упомянутую АСУ ТП на основании произведенных замеров параметров метрик средством мониторинга доступности 230 во время проведения тестирования определенной конфигурации АСУ ТП, имитирующийся на испытательном стенде 210.

Во время анализа полученных данных средство оценки влияния 240 оценивает влияние каждого исследуемого ПО на АСУ ТП и определяет, какие последствия могут произойти в случае заражения АСУ ТП соответствующим исследуемым ПО. Под последствиями также подразумевается, какой будет нанесен ущерб тестируемой конфигурации АСУ ТП и в чем ущерб заключается.

В частном случае реализации оценка имеет вероятностный характер, и определяется диапазоном от 0 до 100. Поэтому при проведении испытаний даже работа компонентов СПА (АСУ ТП) в разрешенных диапазонах дает не нулевую оценку. Это позволяет обнаружить признаки опасности для АСУ ТП даже при работе каждого отдельного компонента в разрешенных рамках, но за счет весовой оценки их совокупность укажет на опасность.

В еще одном частном случае реализации, на основании сделанной оценки средство оценки влияния 240 дополнительно производит формирование рекомендаций. Рекомендации могут содержать сведения следующего характера:

- позволяющие обнаруживать признаки заражения систем АСУ ТП опасным ПО (вредоносным ПО), в том числе без установки специального ПО (например, антивирусного ПО);
- по защите от заражения от вредоносного ПО;
- об устранении заражения или внедрения ПО и его последствий;
- о корректировке компонента АСУ ТП или сетевого трафика (передаваемых данных при взаимодействии компонентов), которые подвержены влиянию исследуемого ПО;
- о проведении дополнительных исследований.

Во время оценки также может производиться определение наиболее опасного вредоносного ПО. Наиболее опасным является ПО, которое оказывает на АСУ ТП необратимые отклонения. Кроме того, на основании серии исследований на ряде конфигураций АСУ ТП средство оценки может сформировать рейтинг опасности, который будет содержать информацию о наиболее опасном вредоносном ПО для технологических систем (сетей).

На Фиг. 3 схематично представлен пример исполнения испытательного стенда, предназначенного для имитации определенной конфигурации СПА, в частности, АСУ ТП.

Предлагаемый вариант испытательного стенда 210 предоставляет необходимую

тестовую инфраструктуру, с помощью которой возможно произвести имитацию определенной конфигурации АСУ ТП для проведения его исследования на уязвимость относительно исследуемого ПО.

Для формирования определенной конфигурации СПА испытательный стенд 210 содержит различные компоненты СПА, из которых подбираются необходимые компоненты для тестирования, и по крайней мере один сервер, с помощью которого формируются необходимые рабочие станции пользователей или виртуальные машины. Указанный сервер может быть реализован как сервер виртуализации (т.е. ESXi) или на физическом аппаратном обеспечении. Стоит отметить, что рабочие станции пользователей и виртуальные машины могут быть взаимозаменяемыми, что зависит от варианта реализации испытательного стенда 210. Испытательный стенд 210 включает также и такие средства, как средство отбора ПО 220, средство мониторинга доступности 230 и средство оценки влияния исследуемого ПО 240. Все элементы стенда 210 объединены технологической сетью, с помощью которой производятся взаимодействия. При этом технологическая сеть может разделяться на несколько сетей. Так, например, на Фиг. 3 условно представлены три сети с помощью сетевых плат (NIC #1, NIC #2 и NIC#3). Сетевая плата (англ. network interface controller/card) также известна как сетевая карта или сетевой адаптер.

Испытательный стенд 210 позволяет осуществлять следующие предварительные действия для осуществления последующего тестирования:

• настройку различных компонентов СПА и хостов на сервере;

• установку различных компонентов СПА на испытательном стенде, подключение СПА и создание потока данных;

• управление и техническое обслуживание компонентов СПА, размещенных в отдельных виртуальных локальных сетях (NIC #1 и NIC #2 соответственно);

• удаленное подключение к компонентам СПА (через NIC#3) для проведения тестирования и исследования в целом.

На Фиг. 4 схематично представлен пример сценария влияния вредоносного ПО на АСУ ТП, при котором происходит отказ в обслуживании. Так, сценарий состоит из 5 основных этапов.

На первом этапе производится внедрение образца вредоносного ПО 420 на рабочую станцию 440, на которой установлен по крайней мере один компонент АСУ ТП. Указанный образец во время своего исполнения производит блокировку рабочей станции или модификацию локального ресурса рабочей станции. Примером локального ресурса является центральный процессор (CPU), оперативная память (RAM), файлы, реестр и т.п. Соответственно под модификацией может пониматься значительное потребление CPU/RAM, изменение памяти процессов, файлов или реестра.

На втором этапе компонент АСУ ТП 460 попытался и не смог получить доступ к локальным ресурсам рабочей станции 440, которые были заблокированы или изменены образцом вредоносного ПО.

На третьем этапе компонент АСУ ТП 460 становится нестабильным (например, зависает или возникает авария в работе) или не может работать должным образом (т.е. контролировать технологический процесс при работе с полевым устройством). Что при водит к отказу в обслуживании 470.

На четвертом этапе средство мониторинга 230 собирает события, произошедшие на предыдущих этапах 1-3.

На пятом этапе средство мониторинга 230 составляет отчет о выявленных аномалиях 480.

Другие сценарии могут включать в себя модификацию нескольких локальных ресурсов (например, конфигурацию операционной системы, конфигурационные файлы приложений и т.д.), которые вызывают некорректную работу компонентов АСУ ТП, блокировку или модификацию сетевых ресурсов (например, DoS сетевого оборудования и ПЛК).

Средство мониторинга 230 может быть разработано, например, как с использованием фреймворка анализа производительности Windows Performance Analysis (WPA), так и на пользовательских драйверах фильтров, что позволяет обнаруживать широкий спектр событий.

На Фиг. 5 показана блок-схема, иллюстрирующая способ оценки влияния исследуемого ПО на компоненты промышленной системы. Представленный способ реализуется с помощью средств системы, описанной на Фиг. 2.

На этапе 510 производят отбор образцов исследуемого ПО, которые потенциально способны нанести ущерб системе промышленной автоматизации (СПА) и, в частности, системе промышленного контроля (СПК). Отбор производится путем запуска и исполнения каждого ПО в изолированной среде типа «песочница». Во время исполнения формируется журнал событий, содержащий все активности, произошедшие во время исполнения. На основании анализа журнала событий производят отбор исследуемого ПО подходящего для тестирования на испытательном стенде 210. Так, отбор образцов может осуществляться при помощи ряда критериев, которые указывают как говорилось выше на воздействия, представляющие угрозу доступности или работоспособности, а также целостности конфигурации СПА.

На этапе 530 производят автоматизированное исследование воздействия отобранных образцов исследуемого ПО на определенную конфигурацию СПА с помощью испытательного стенда 210. Исследование заключается в проведении по крайней мере одного испытания, которое направлено на сбор данных о влиянии исследуемого ПО на тестируемую конфигурацию СПА, имитирующийся на стенде 210. Количество испытаний зависит от количества исследуемого ПО. Во время каждого испытания производится внедрения образца исследуемого ПО в тестируемую конфигурацию СПА и в проведении определенного информационного обмена данными между компонентами тестируемую конфигурацию СПА. Информационный обмен данными определяется согласно самим компонентам конфигурации и задачам, которые должны выполнять указанные компоненты. Во время каждого испытания производят фиксацию всех выявленных причин и/или событий, приводящих к нарушению функционирования стенда, имитирующего конфигурацию СПА. Примером нарушения может быть любое отклонение в работе компонента конфигурации СПА, приводящее к отказу в обслуживании этого компонента или всей конфигурации СПА в целом.

На этапе 550 производят анализ всех выявленных причин и событий, приводящих к нарушению функционирования определенной конфигурации СПА.

На этапе 570 на основании анализа определяют степень влияния проанализированного исследуемого ПО на определенную конфигурации СПА, а также возможную деградацию вычислительных ресурсов определенной конфигурации СПА, имитируемой на испытательном стенде 210.

На Фиг. 6 показана блок-схема, иллюстрирующая частный случай реализации представленного способа на Фиг. 5, а именно, способ оценки влияния вредоносного ПО, которое вызывает отказ в обслуживание компонентов определенной конфигурации СПА. Представленный способ реализуется с помощью системы, описанной на Фиг. 2. Предположим, что требуется произвести тестирование определенной конфигурации

СПА для оценки влияния на нее вредоносного ПО, т.е. какова устойчивость СПА. Для этого на испытательный стенд производят передачу спецификации, которая содержит сведения о компонентах СПА и их функциональных возможностях. Кроме того, спецификация может содержать и сведения о том, как производятся взаимодействия между компонентами или какой производится обмен данными. Такие сведения актуальны в случае, когда компоненты конфигурации СПА были модифицированы и производят нестандартные для них взаимодействия.

На этапе 610 формируют на испытательном стенде определенную конфигурацию СПА согласно полученной спецификации для проведения тестирования. Под формированием подразумевается подключение или отключение определенных компонентов (устройств) для полного соответствия полученной спецификации.

На этапе 620 получают набор исследуемого ПО, где набор включает по крайней мере образ одного вредоносного ПО. Так как вредоносного ПО огромное количество, то поэтому получаемый набор исследуемого ПО может предварительно ограничиваться. Например, ограничения могут основываться на популярности образцов вредоносного ПО или степени угрозы. Кроме того, набор исследуемого ПО может предварительно отбираться на дополнительном этапе 615 и соответствовать определенному виду устройств или оборудования, являющихся компонентами тестируемой конфигурацию СПА. В частном случае реализации, на этапе 615 отбор производят на основании анализа вредоносного ПО в имитируемой среде типа «песочница» с последующим формированием журнала событий. Далее анализируют журнал событий каждого образца вредоносного ПО, производят выборку подходящего вредоносного ПО для тестирования.

В одном из вариантов реализации выборка вредоносного ПО осуществляется при помощи ряда критериев, которые указывают на воздействия, представляющие угрозу доступности или работоспособности, а также целостности для соответствующей определенной конфигурации СПА.

На этапе 630 выполняют тестирование сформированной конфигурации СПА на испытательном стенде при помощи полученного набора. Во время тестирования производят информационный обмен данными между компонентами конфигурации СПА в рамках определенного испытания. Испытание содержит сценарий, в соответствии с которым производится указанный обмен данными при тестировании. Кроме того, сценарий учитывает и использование в рамках тестирования образцов вредоносного ПО.

На этапе 640 во время проведения испытаний выявляют случаи отказа в обслуживании компонентов, из которых состоит стенд, имитирующий определенную конфигурацию СПА.

На этапе 650 производят анализ всех выявленных причин и событий, связанных с выявленными отказами в обслуживании, что указывает на нарушение функционирования стенда, имитирующего определенную конфигурацию СПА.

На этапе 660 определяют влияние вредоносного ПО на определенную конфигурацию СПА, а также степень деградации производительности определенной конфигурации СПА.

На этапе 680 выносят решение об опасности определенного вредоносного ПО для определенной конфигурации СПА на основании определенного влияния соответствующего вредоносного ПО.

На этапе 690 дополнительно выявляют компрометирующие признаки, влияющие на сбой в работе определенной конфигурации СПА. При этом этапы 680 и 690 могут быть

также взаимозаменяемыми.

Фиг. 7 представляет пример компьютерной системы 20 общего назначения, которая может быть использована как компьютер клиента (например, персональный компьютер) или сервер, представленные на Фиг. 2. Компьютерная система 20 содержит 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 компьютерной системы 20, например, в момент загрузки операционной системы с использованием ПЗУ 24.

Компьютерная система 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 компьютерной системы 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.

Компьютерная система 20 способна 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 компьютерной системы 20, представленного на Фиг. 7. 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 компьютерная система (персональный компьютер) 20 подключена 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. Специалисту в данной области становится понятным, что могут существовать и другие варианты осуществления настоящего изобретения, согласующиеся с сущностью и объемом настоящего изобретения.

(57) Формула изобретения

1. Испытательный стенд мониторинга, контроля и анализа для оценки влияния образцов вредоносного ПО на функционирование определенной конфигурации системы промышленной автоматизации (СПА), при этом испытательный стенд получает спецификацию определенной конфигурации СПА и, по крайней мере, один образец вредоносного ПО и включает:

а) изменяемый набор различных компонентов СПА,

б) средство мониторинга доступности, предназначенное для контроля проводимого автоматизированного тестирования определенной конфигурации СПА, где во время указанного тестирования средство мониторинга доступности выявляет влияние каждого образца исследуемого ПО на доступ к каждому компоненту, содержащемуся в тестируемой СПА, или на определенную конфигурацию СПА в целом на основании снимаемых параметров метрик, актуальных для тестируемой конфигурации СПА; и

в) средство оценки влияния, предназначенное для оценки степени влияния исследуемого ПО на упомянутую СПА на основании произведенных замеров средством мониторинга доступности параметров метрик, которые позволяют оценить производительность и временные сбои в работе компонентов СПА, во время проведения тестирования определенной конфигурации СПА.

2. Испытательный стенд по п. 1, отличающийся тем, что дополнительно включает средство отбора вредоносного ПО.

3. Испытательный стенд по п. 2, отличающийся тем, что средство отбора вредоносного ПО производит отбор образов вредоносного ПО на основании исследования исполнения различного ПО в изолированной среде с последующим анализом сформированного журнала активностей по итогам исследования для выявления воздействий, представляющих потенциальную угрозу функциональности

СПА.

4. Испытательный стенд по п. 1, отличающийся тем, что имеет доступ в информационно-коммуникационную сеть для удаленного взаимодействия.

5. Испытательный стенд по п. 1, отличающийся тем, что нарушением функционирования испытательного стенда, имитирующего определенную конфигурацию СПА, является по крайней мере выявление события, указывающего на отказ в обслуживание по крайней мере одного компонента СПА.

6. Испытательный стенд по п. 1, отличающийся тем, что средство оценки влияния дополнительно производит формирование рекомендаций.

7. Испытательный стенд по п. 1, отличающийся тем, что рекомендации содержат по крайней мере одно из следующих сведений:

• позволяющие обнаруживать признаки заражения СПА вредоносным ПО, в том числе без установки антивирусного ПО;

• по защите от заражения от вредоносного ПО;

• об устранении заражения и его последствий;

• о корректировке компонента СПА или сетевого трафика, которые подвержены влиянию вредоносного ПО;

• о проведении дополнительных исследований.

8. Способ оценки влияния вредоносного ПО на работоспособность системы промышленной автоматизации (СПА), реализующийся при помощи испытательного стенда по п. 1 и заключающийся в том, что:

а) формирует на испытательном стенде определенную конфигурацию инфраструктуры СПА согласно полученной спецификации, которая включает состав и задачи компонентов СПА;

б) получает набор образцов вредоносного ПО;

в) выполняет тестирование полученного набора на сформированном испытательном стенде, во время которого производят выявление причин и событий, приводящих к нарушению функционирования компонентов СПА и полевых элементов, за которые отвечает компоненты СПА, при этом тестирование включает определенный сценарии работы компонентов СПА, где во время указанного тестирования выявление причин и событий проводится на основании снимаемых параметров метрик, актуальных для тестируемой конфигурации СПА;

г) производит анализ выявленных причин и событий, приводящих к нарушению функционирования компонентов СПА на испытательном стенде на основании произведенных замеров параметров метрик, которые позволяют оценить производительность и временные сбои в работе компонентов СПА;

д) определяет влияние вредоносного ПО на конфигурацию СПА.

9. Способ по п. 8, в котором инфраструктура СПА представляет собой как сетевое оборудование и компьютер пользователя (оператора), так различные компоненты автоматизированных систем управления технологическими процессами (АСУ ТП).

10. Способ по п. 8, в котором компонентами СПА по крайней мере являются системы диспетчерского управления и сбора данных, распределенные системы управления, системы противоаварийной защиты, системы на программируемых логических контроллерах и шлюзы данных.

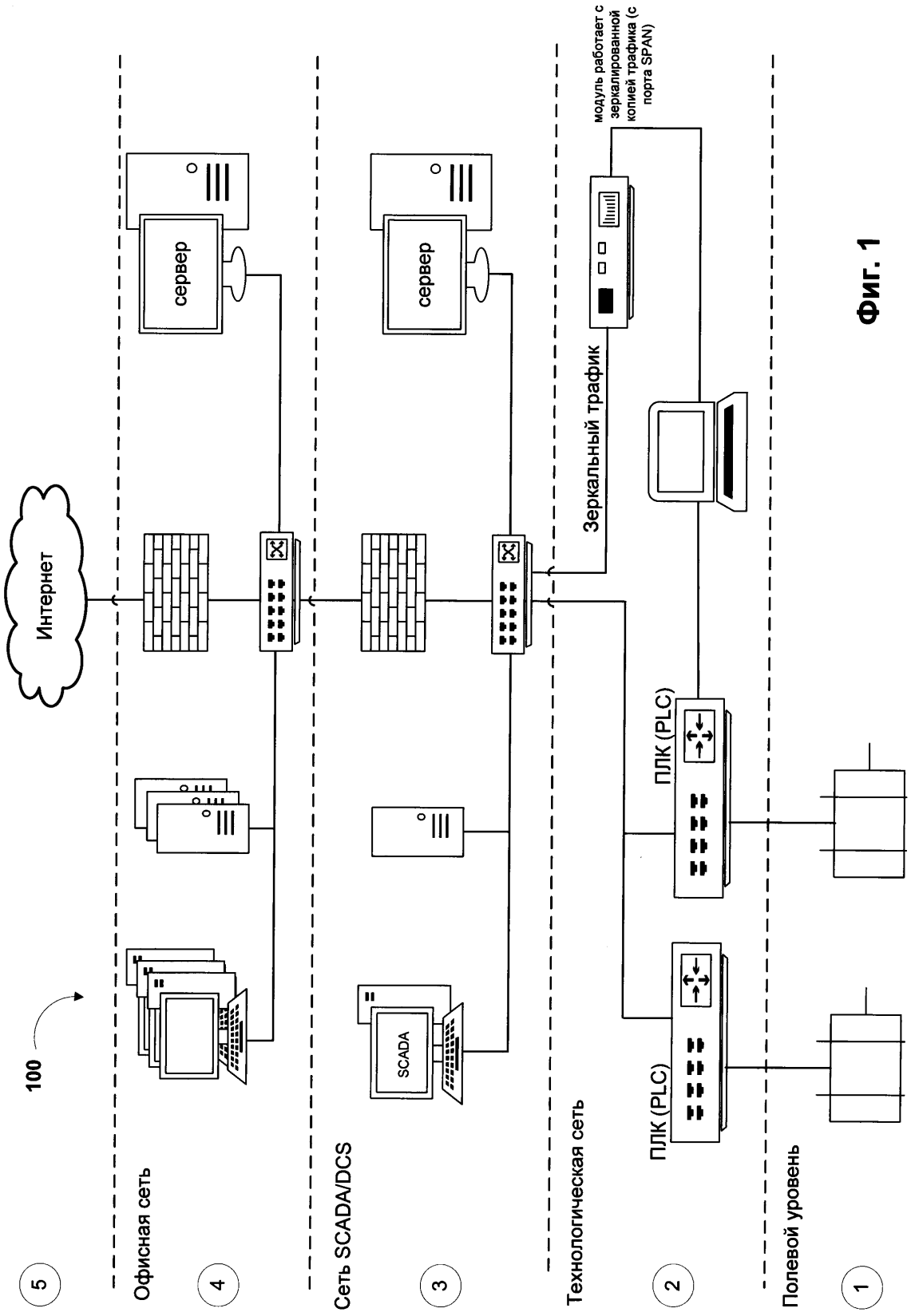
11. Способ по п. 8, в котором формируют испытательный стенд путем виртуализации.

12. Способ по п. 8, в котором формируют испытательный стенд путем включения в единую сеть только тех компонентов, которые входят в состав конфигурации инфраструктуры СПА согласно спецификации.

13. Способ по п. 8, в котором дополнительно получаемый набор образцов вредоносного ПО был сформирован на основании анализа вредоносного ПО в имитируемой среде типа «песочница» с последующим выявлением подходящего вредоносного ПО для тестирования определенной конфигурации инфраструктуры СПА.

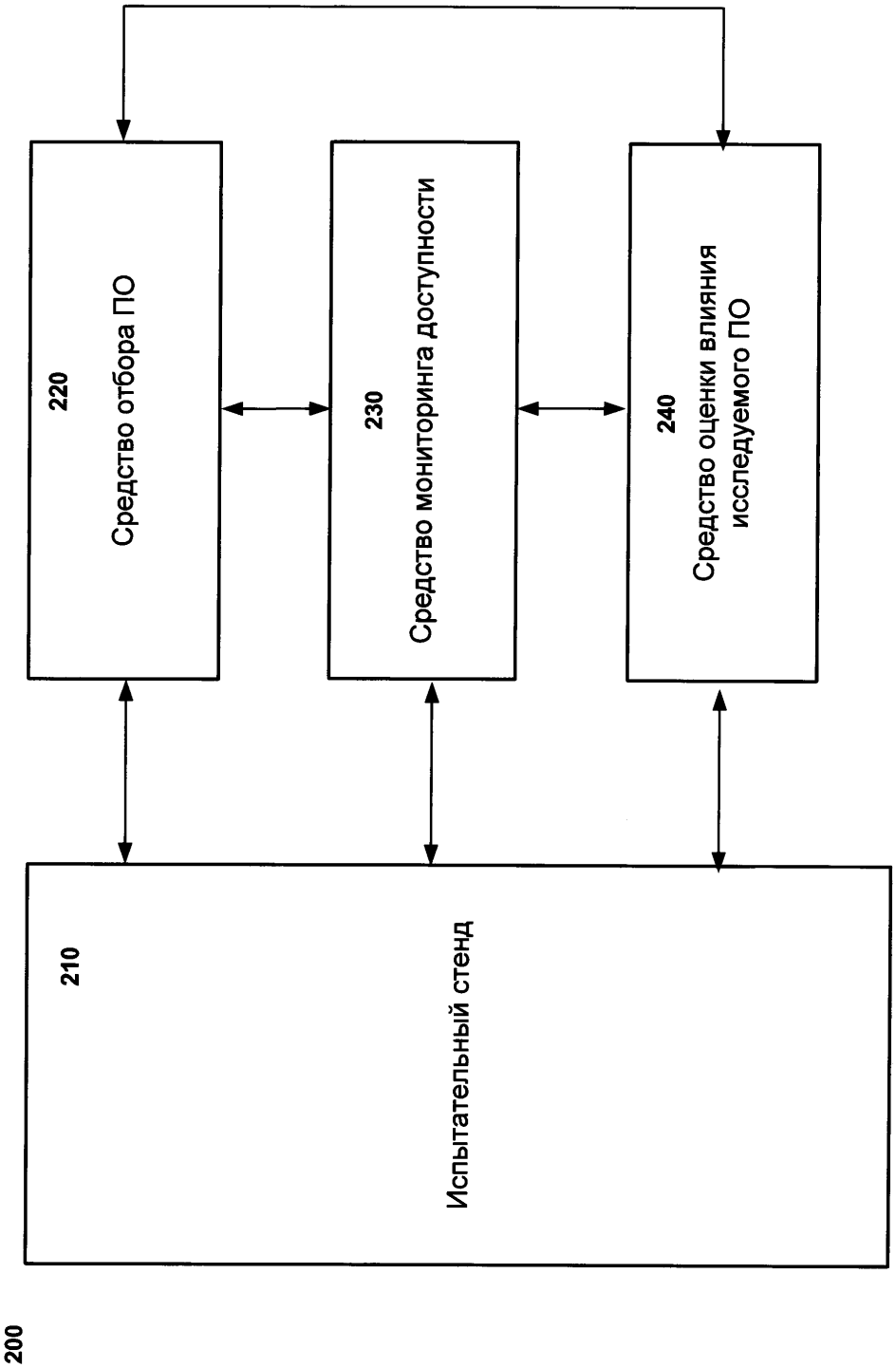
14. Способ по п. 8, в котором дополнительно на шаге д) определяет степень влияния вредоносного ПО на СПА, где степень указывает на критичность вредоносного ПО в отношении к конфигурации СПА.

1


Интернет
сервер
сервер
SCADA
модуль работает с зеркалированной копией трафика (с порта SPAN)
Зеркальный трафик
ПЛК (PLC)
ПЛК (PLC)
100
5
Офисная сеть
4
Сеть SCADA/DCS
3
Технологическая сеть
2
Полевой уровень
1

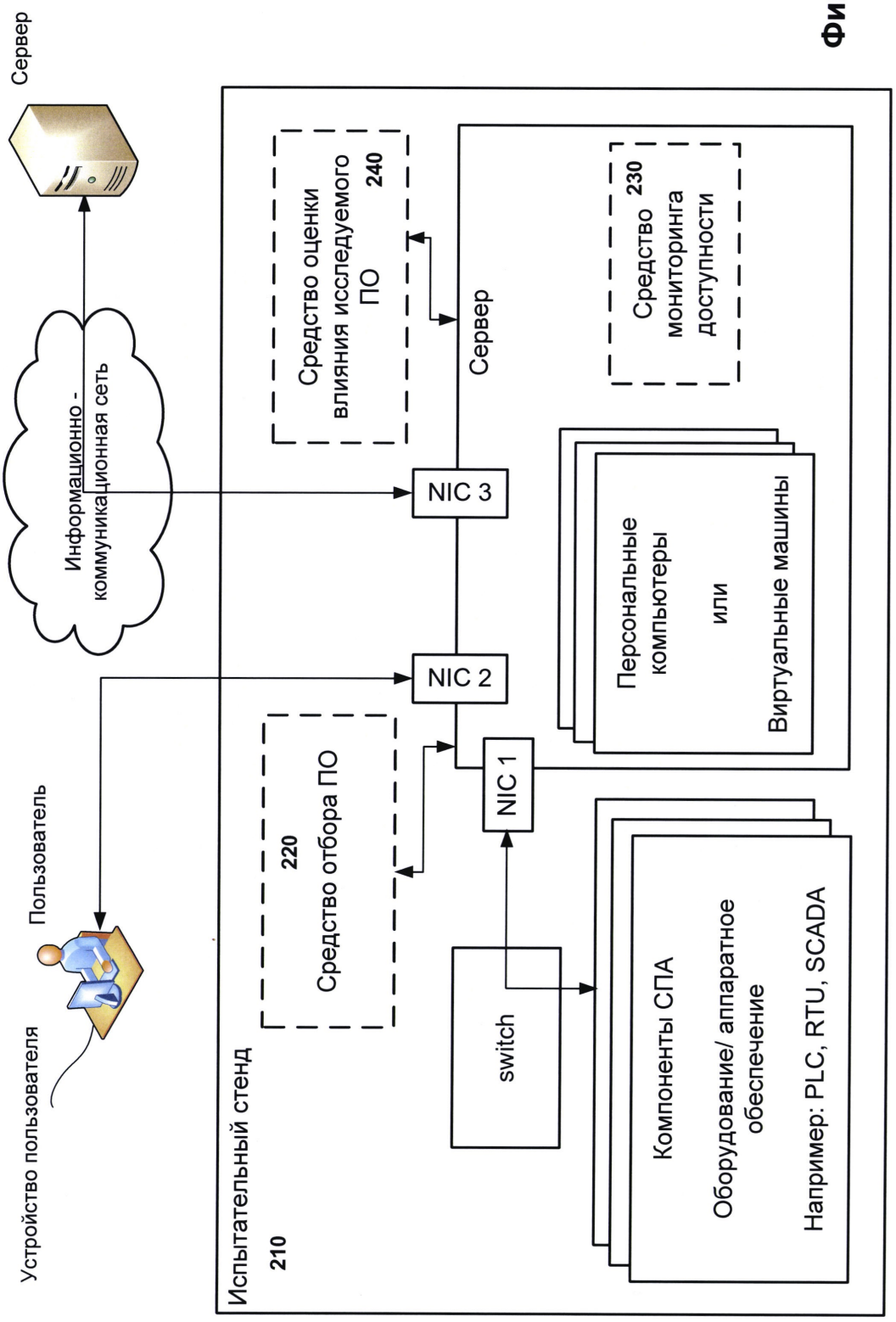
Фиг. 1

2

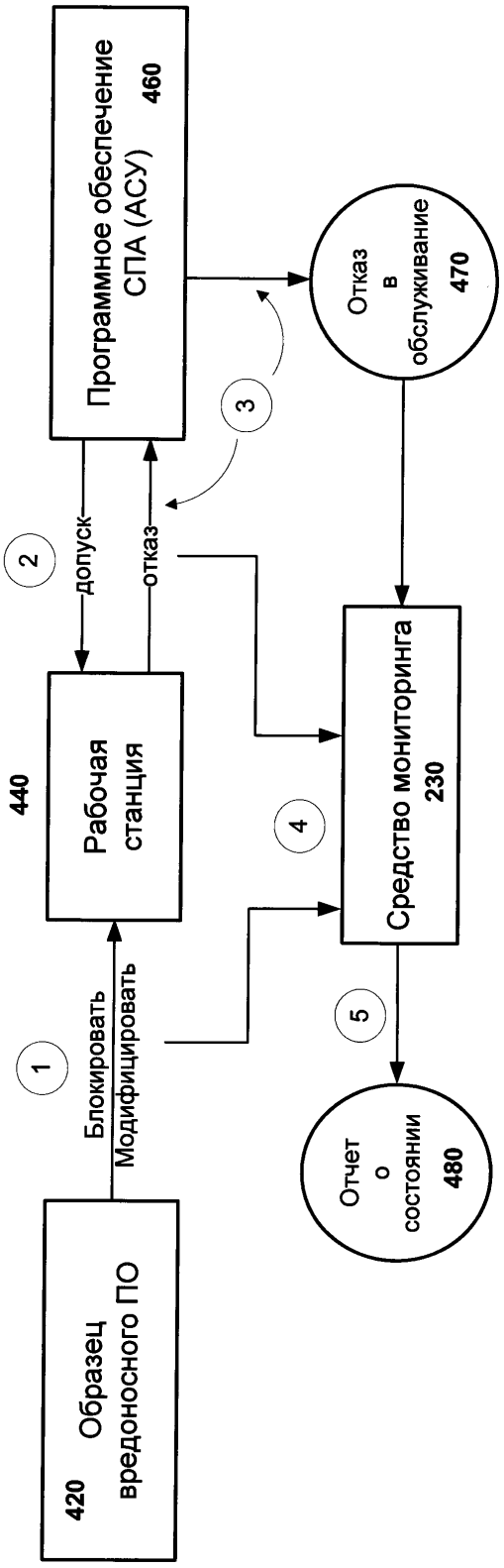

220
Средство отбора ПО
230
Средство мониторинга доступности
240
Средство оценки влияния исследуемого ПО
210
Испытательный стенд
200

Фиг. 2

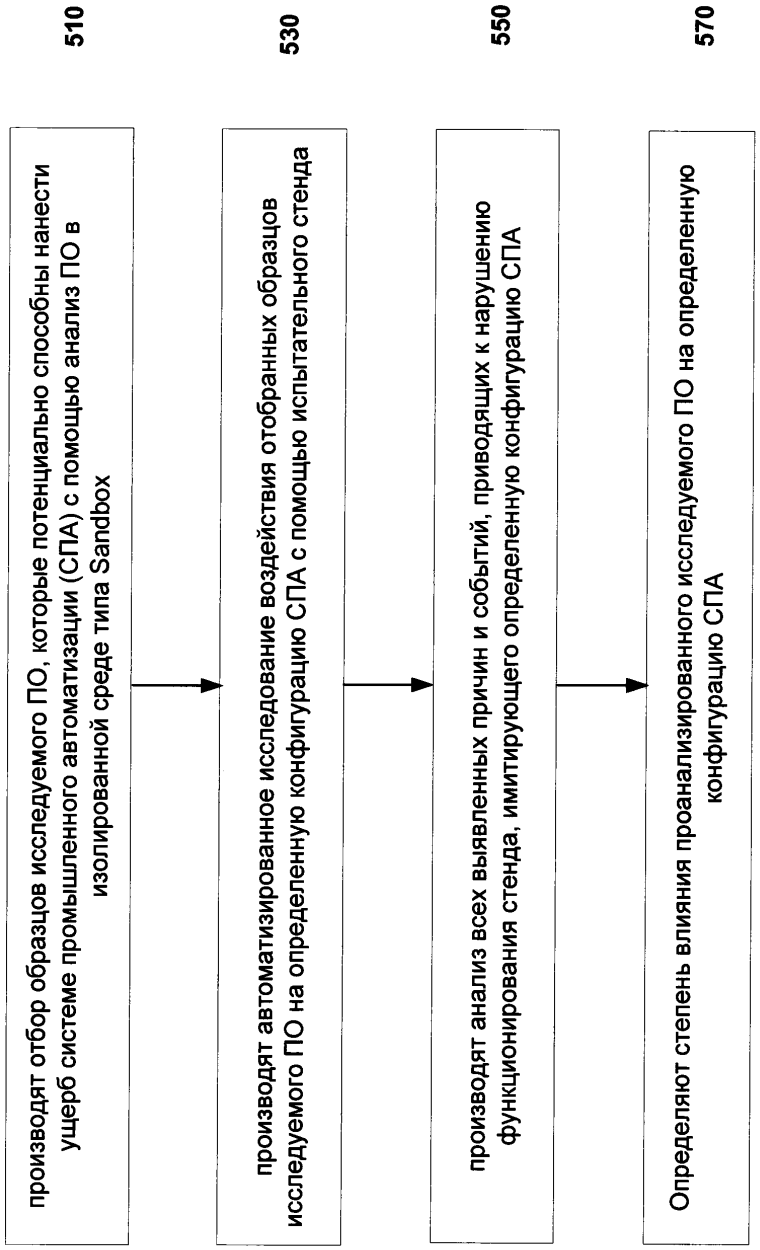
3


Сервер
Информационно - коммуникационная сеть
Пользователь
Устройство пользователя
Испытательный стенд
210
220
Средство отбора ПО
Средство оценки влияния исследуемого ПО
240
Сервер
Средство мониторинга доступности
230
NIC 3
NIC 2
NIC 1
Персональные компьютеры
или
Виртуальные машины
switch
Компоненты СПА
Оборудование/ аппаратное обеспечение
Например: PLC, RTU, SCADA

Фиг. 3

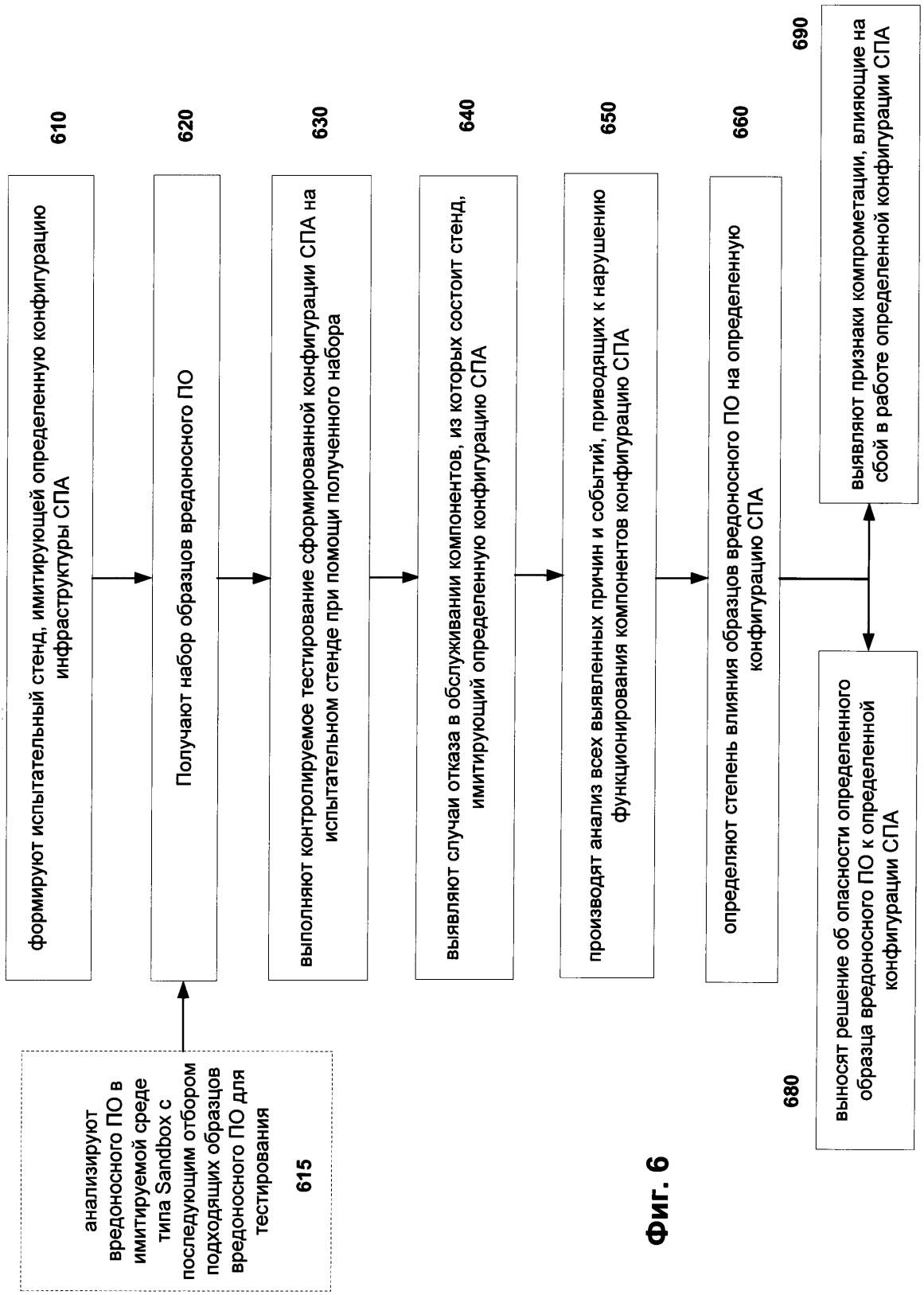

Программное обеспечение СПА (АСУ) 460
Отказ в обслуживание 470
3
2
допуск
отказ
440
Рабочая станция
4
Средство мониторинга 230
1
Блокировать
Модифицировать
5
Отчет о состоянии 480
420
Образец вредоносного ПО

Фиг. 4


510
производят отбор образцов исследуемого ПО, которые потенциально способны нанести ущерб системе промышленного автоматизации (СПА) с помощью анализ ПО в изолированной среде типа Sandbox
530
производят автоматизированное исследование воздействия отобранных образцов исследуемого ПО на определенную конфигурацию СПА с помощью испытательного стенда
550
производят анализ всех выявленных причин и событий, приводящих к нарушению функционирования стенда, имитирующего определенную конфигурацию СПА
570
Определяют степень влияния проанализированного исследуемого ПО на определенную конфигурацию СПА

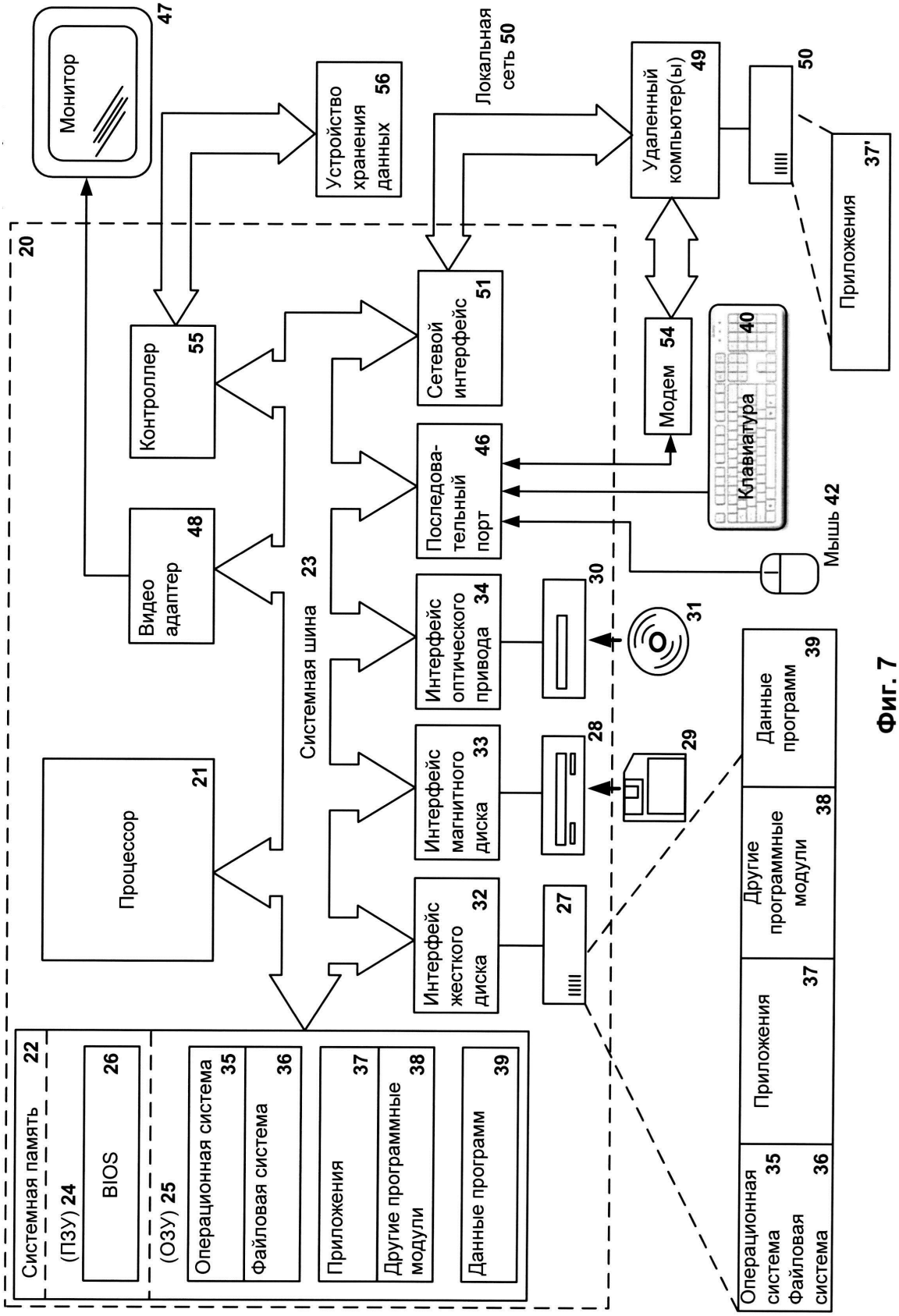
Фиг. 5

6


610
формируют испытательный стенд, имитирующей определенную конфигурацию инфраструктуры СПА
620
Получают набор образцов вредоносного ПО
630
выполняют контролируемое тестирование сформированной конфигурации СПА на испытательном стенде при помощи полученного набора
640
выявляют случаи отказа в обслуживании компонентов, из которых состоит стенд, имитирующий определенную конфигурацию СПА
650
производят анализ всех выявленных причин и событий, приводящих к нарушению функционирования компонентов конфигурацию СПА
660
определяют степень влияния образцов вредоносного ПО на определенную конфигурацию СПА
690
выявляют признаки компрометации, влияющие на сбой в работе определенной конфигурации СПА
680
выносят решение об опасности определенного образца вредоносного ПО к определенной конфигурации СПА
615
анализируют вредоносного ПО в имитируемой среде типа Sandbox с последующим отбором подходящих образцов вредоносного ПО для тестирования

Фиг. 6

7


Монитор 47
Устройство хранения данных 56
Локальная сеть 50
Удаленный компьютер(ы) 49
50
Приложения 37'
20
Контроллер 55
Сетевой интерфейс 51
Модем 54
Клавиатура 40
Последова-тельный порт 46
Мышь 42
Видео адаптер 48
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 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39

Фиг. 7