РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 753 169**(13) **C1**

(51) МПК
*G06N 7/00* (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

# (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
*G06N 7/00 (2021.05)*

(21)(22) Заявка: **2020142565, 23.12.2020**

(24) Дата начала отсчета срока действия патента:
**23.12.2020**

Дата регистрации:
**12.08.2021**

Приоритет(ы):
(22) Дата подачи заявки: **23.12.2020**

(45) Опубликовано: **12.08.2021** Бюл. № **23**

Адрес для переписки:
**195251, Санкт-Петербург, ул. Политехническая, 29, Центр интеллектуальной собственности и трансфера технологий ФГАОУ ВО "СПбПУ"**

(72) Автор(ы):
**Калинин Максим Олегович (RU),**
**Лаврова Дарья Сергеевна (RU),**
**Павленко Евгений Юрьевич (RU)**

(73) Патентообладатель(и):
**федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого" (ФГАОУ ВО "СПбПУ") (RU)**

(56) Список документов, цитированных в отчете о поиске: **МАКСИМОВСКИЙ А.Ю.: "Спектральные и комбинаторные свойства редуцированных графов де Брейна", Вопросы кибербезопасности, 2018.N4(28), стр. 70-76 [найдено: 05.07.2021] Найдено в: "https://cyberleninka.ru/article/n/spektralnye-i-kombinatoryne-svoystva-redutsirovannyh-grafov-de-breyna". МАКСИМОВСКИЙ А.Ю. "О применении теоретико-групповых и** (см. прод.)

## (54) Способ саморегуляции сетевой инфраструктуры промышленных объектов при воздействии угроз безопасности

(57) Реферат:

Изобретение относится к области компьютерных систем, а именно к сетевой инфраструктуре современных промышленных объектов и способам ее автоматического перестроения при обнаружении угроз безопасности. Техническим результатом заявленного решения является повышение мобильности и производительности сети, а также возможность нейтрализации угроз безопасности. Технический результат достигается за счет того, что в заявленном решении осуществляют перестроение сети при получении сигнала от системы обнаружения угроз безопасности, для чего формируют целевую функцию промышленного объекта, графовое представление сетевой инфраструктуры промышленного объекта, наборы связей и операций между кластерами каждой функции из набора функциональных последовательностей, полученные с использованием графов де Брёйна, и при получении сигнала обнаружения угроз безопасности составляют список нарушенных функций из набора функциональных последовательностей, затем выбирают наиболее быстрый для применения вариант перестроения сетевой структуры и применяют к текущей структуре сети. 5 ил.

RU 2753169 C1

RU 2753169 C1

(56) (продолжение):
комбинаторных методов мониторинга информационной безопасности сложных систем", Тринадцатая международная конференция "Управление развитием крупномасштабных систем" (MLSD'2020) Россия, Москва, ИПУ РАН, 28-30 сентября 2020 г., [найдено: 05.07.2021] Надено в: "https://mlsd2020.ipu.ru/ru/prcdngs". TEKINER FIRAT et al.: "Implementation and evaluation of shufflenet, gemnet and de bruijn graph logical network topologies", 2004, [найдено: 05.07.2021] Надено в: "http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.62.3677&rep=rep1&type=pdf";. US 8600951 B2, 03.12.2013. US 7117257 B2, 03.10.2006.

RU 2753169 C1

RU 2753169 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 753 169**(13) **C1**

(51) Int. Cl.
*G06N 7/00* (2006.01)

## (12) ABSTRACT OF INVENTION

(52) CPC
*G06N 7/00 (2021.05)*

(21)(22) Application: **2020142565, 23.12.2020**

(24) Effective date for property rights:
**23.12.2020**

Registration date:
**12.08.2021**

Priority:
(22) Date of filing: **23.12.2020**

(45) Date of publication: **12.08.2021** Bull. № **23**

Mail address:
**195251, Sankt-Peterburg, ul. Politekhnicheskaya, 29, Tsentr intellektualnoj sobstvennosti i transfera tekhnologij FGAOU VO "SPbPU"**

(72) Inventor(s):
**Kalinin Maksim Olegovich (RU),**
**Lavrova Darya Sergeevna (RU),**
**Pavlenko Evgenij Yurevich (RU)**

(73) Proprietor(s):
**federalnoe gosudarstvennoe avtonomnoe obrazovatelnoe uchrezhdenie vysshego obrazovaniya "Sankt-Peterburgskij politekhnicheskij universitet Petra Velikogo" (FGAOU VO "SPbPU") (RU)**

### (54) METHOD FOR SELF-REGULATION OF NETWORK INFRASTRUCTURE OF INDUSTRIAL FACILITIES UNDER INFLUENCE OF SECURITY THREATS

(57) Abstract:

FIELD: computer systems.

SUBSTANCE: invention relates to the field of computer systems, namely to the network infrastructure of modern industrial facilities and methods for its automatic rebuilding upon detection of security threats. The effect is achieved due to the fact that in the claimed solution the network is rebuilt upon receipt of a signal from the security threat detection system, for which the target function of the industrial facility is formed, the graphical representation of the network infrastructure of the industrial facility, sets of connections and operations between clusters of each function from a set of functional sequences, obtained using de Bruijn graphs, and upon receipt of a security threat detection signal, compile a list of violated functions from a set of functional sequences, then choose the fastest option for rebuilding the network structure to apply and apply to the current network structure.

EFFECT: increased mobility and performance of the network, as well as the ability to neutralize security threats.

1 cl, 5 dwg

RU 2753169 C1

RU 2753169 C1

Изобретение относится к области компьютерных систем, а именно к сетевой инфраструктуре современных промышленных объектов и способам ее автоматического перестроения при воздействии угроз безопасности.

Технической проблемой является повышение скорости реагирования на угрозы безопасности и повышение защищенности сетевой инфраструктуры промышленных объектов за счет перестроения сетевой инфраструктуры на этапе обнаружения угрозы безопасности таким образом, чтобы угроза безопасности не могла быть реализована.

Известен способ, обеспечивающий выполнение адаптивной аналитики кибербезопасности системы (патент США №US9032521B2, опубликован 12.05.2015, МПК H04L63/1433). На компьютере вычисляется оценка кибербезопасности системы, зависимая от уровня текущей сетевой активности. Полученная оценка указывает на вероятность нарушения безопасности в системе и позволяет сформировать сигнал о подозрительной сетевой активности, если оценка переходит установленные границы, свидетельствующие о нарушении. Недостатком данного решения является его ориентированность на косвенное обнаружение угроз безопасности по вычислимой оценке, которая определяется на основании признаков сетевой активности в системе. Тем самым изобретение позволяет сигнализировать об угрозе, а не о нарушении, а также не позволяет нейтрализовать угрозы безопасности (согласно п. 1 формулы). Адаптация системы заключается в выполнении автоматического обновления программных компонентов и связана только с использованием вычислительной модели оценки, реагирующей на признаки того, является ли нарушение безопасности настоящей угрозой или нет. При этом все действия по нейтрализации выявленных угроз безопасности выполняются человеком.

Известно изобретение, представляющее собой систему кибербезопасности, реализующую агрегирование данных, поступающих от множества узлов сети, выявление инцидента безопасности и перестроение рабочих процессов в ответ на выявленный инцидент безопасности (патент США №20200244696, опубликован 07.30.2020, МПК H04L29/06; H04L9/00; H04L9/32). В зависимости от характера конкретного инцидента безопасности решение позволяет инициировать план действий, адаптированный к операционному центру безопасности и его операционным процедурам для защиты узлов сети, затронутых инцидентом безопасности.

Согласно п. 1 формулы, данное изобретение выполняет идентификацию автоматического действия для устранения угрозы безопасности и инициирует по крайней мере одно автоматическое действие для устранения инцидента безопасности. Согласно п. 2 формулы, по крайней мере одно автоматизированное действие, выполняемое изобретением, блокирует вредоносный сетевой трафик, по крайней мере, в пределах контролируемого сегмента сети. Таким образом, реагируя на инцидент безопасности и блокируя трафик, изобретение перестраивает сетевую инфраструктуру при обнаружении инцидентов безопасности, сохраняя при этом автономность от оператора. Недостатками данного изобретения являются минимальный набор действий по устранению угрозы безопасности, выполняемых автономно от оператора, а также использование политики сетевой безопасности, что недостаточно для регуляции сетевой инфраструктуры промышленных объектов. Это связано с большим масштабом таких объектов, а также с разнородностью типов сетей, входящих в состав сетевой инфраструктуры промышленных объектов (клиент-серверные сети, сенсорные сети, децентрализованные сети, одноранговые сети мобильных устройств).

Наиболее близким техническим решением является способ адаптивной переконфигурации коммуникационной сети устройств (патент США №US7117257B2,

опубликован 03.10.2006, МПК H04Q3/0083). Техническое решение, согласно п. 7 формулы, включает сетевое устройство для адаптивной переконфигурации сети, имеющей не менее одного центрального узла и множество граничных узлов. Устройство реализует временную блокировку граничных узлов, группировку граничных узлов в соответствии с задержкой реконфигурации каждого граничного узла, назначение порога задержки реконфигурации для каждой группы граничных узлов и периодическую перенастройку маршрутов, связанных с граничными узлами в каждой группе граничных узлов в соответствии с указанным порогом задержки. Данное решение обеспечивает быструю переконфигурацию сетевых маршрутов, связывающих взаимодействующие через сеть узлы, где любые два граничных узла могут соединяться между собой через центральный узел. Для повышения адаптивности, мобильности и производительности сети граничные узлы, связанные через центральный узел, разделяются на множество групп на основе оценки временных задержек приема-передачи при взаимодействии с центральным узлом. Это позволяет отделить короткие маршруты от длинных, и в свою очередь, заменяя разные отрезки маршрута на коротких дистанциях, позволяет настраивать короткие маршруты чаще, чем длинные маршруты, тем самым обеспечивая адаптацию пропускной способности сети к изменяющимся условиям. Однако, указанное решение обладает рядом недостатков. Разделение узлов сети осуществляется только по критерию, формируемому на основе оценки задержек при передаче пакетов между граничным узлом и центральным узлом и не учитывает всю сеть в целом. Такой критерий переконфигурации эффективен для небольшой сети с выраженным центральным узлом, через который взаимодействуют граничные узлы. Для такой сети выигрыш в пропускной способности достигается за счет перестроения сетевых маршрутов от граничных узлов к центральному. Однако такой способ неэффективен в случаях децентрализованной и одноранговой сетевых инфраструктур. Целесообразно введение критерия переконфигурации сети, учитывающего набор функций, выполняемых отдельными узлами сетевой инфраструктуры, их связи друг с другом, а также вычислительную мощность узлов сети, поскольку в сетевой инфраструктуре промышленных объектов часто используются малоресурсные сетевые узлы: датчики и контроллеры устройств.

Кроме того, изобретение не ориентировано на нейтрализацию угроз безопасности. Изобретение направлено на повышение мобильности и производительности сети, в то время как для решения задачи нейтрализации угроз безопасности важны не только производительность, но и исключение скомпрометированных узлов сети, а также построение альтернативных путей между узлами, связь между которыми была нарушена в результате воздействия киберугрозы. При этом в указанном решении используется фиксированный (задаваемый) порог задержки. Перестроение сетевой инфраструктуры часто приводит к тому, что узлы, которые ранее были практически не загружены, становятся загруженными и требуют обновления порога задержки для обеспечения адекватной реакции на изменение условий работы сетевой инфраструктуры.

Решение поставленной технической проблемы обеспечивается тем, что в способе саморегуляции сетевой инфраструктуры промышленных объектов при воздействии угроз безопасности определяют целевую функцию рассматриваемого промышленного объекта, выделяя множество физических процессов объекта и набор информационных функций, выполняемых узлами сетевой инфраструктуры объекта, и представляя целевую функцию в виде набора функциональных последовательностей, затем сохраняют целевую функцию в виде набора функциональных последовательностей в базу данных, расположенную на сервере баз данных, затем строят граф сетевой инфраструктуры промышленного объекта и сохраняют его в базу данных, расположенную на сервере

баз данных, затем формируют для каждой функции, входящей в состав целевой функции, кластер, представляющий собой множество, в котором будут собраны все вершины и подграфы графа, способные выполнить данную функцию, строят граф всех возможных вариантов реализации целевой функции в виде многоуровневого графа и сохраняют его в базу данных, расположенную на сервере баз данных, затем, используя графы де Брёйна, получают наборы связей между кластерами и операций между кластерами в связи со строгим порядком при выполнении и взаимосвязи функций, входящих в целевую, затем сохраняют полученные наборы связей и операций между кластерами в базу данных, расположенную на сервере баз данных, затем получают сигнал от системы или модуля обнаружения угроз безопасности о том, какой узел графа затронут воздействием угрозы безопасности, затем определяют список нарушенных функций, которые выполнял затронутый нарушением безопасности узел графа, затем перестраивают инфраструктуру сети промышленного объекта таким образом, чтобы нейтрализовать влияние угрозы с использованием кластеров функций, наборов связей и операций между кластерами, многоуровневого графа, затем проверяют, что целевая функция снова выполняется узлами.

Сетевая инфраструктура представляется в виде ориентированного графа, а ее целевая функция (набор необходимых функций промышленного объекта) – в виде последовательности взаимосвязанных функций, ассоциированных с узлами графа. Воздействие угрозы безопасности представляется в виде изменения числа узлов и дуг графа, а также изменения их характеристик. Для каждой функции, входящей в состав целевой, формируется кластер – набор узлов и подграфов графа, которые способны выполнить эту же функцию и заменить устройство, выполняющее функцию в данный момент, в случае его выхода из строя или компрометации в результате реализации угрозы безопасности в виде нарушения безопасности.

Для целевой функции задаются связи между кластерами с использованием графов де Брёйна. Использование графов де Брёйна позволяет выделить между разными кластерами такие узлы или подграфы, связь между которыми может быть построена максимально быстро, так как будут найдены подграфы, заканчивающиеся (для первого кластера) и начинающиеся (для второго) с одного и того же узла графа, что минимизирует время соединения и выполнения обеих функций, и, следовательно, обеспечит максимально быстрое построение альтернативной функциональной последовательности, эквивалентной целевой функции, наблюдаемой до начала реализации угрозы безопасности.

Способ саморегуляции сетевой инфраструктуры промышленных объектов при воздействии угроз безопасности поясняется изображением связи между кластерами с использованием графа де Брёйна (фиг. 1), общей схемой осуществления саморегуляции сетевой инфраструктуры промышленного объекта (фиг. 2), а также примером, включающим три фигуры (граф сетевой инфраструктуры до воздействия угрозы безопасности (фиг. 3), построение новых связей с помощью графов де Брёйна (фиг. 4), новый граф сетевой инфраструктуры после выполнения саморегуляции (фиг. 5)).

Последствия воздействия угрозы безопасности в терминах графовой модели представлены в виде разрывов в функциональной последовательности целевой функции промышленного объекта. Например, для объекта, реализующего целевую функцию $F = f_6(f_5(f_4(f_3 + f_2[f_1])))$, в результате нарушения безопасности из строя выведен узел, реализующий функцию $f_4$. Тогда в результате разрыва функции $F$ остались две последовательности: $f_6(f_5)$ и $f_3 + f_2[f_1]$, для соединения которых необходимо найти

нескомпрометированный узел, способный выполнять функцию $f_4$ и взаимодействовать с узлами, реализующими две оставшиеся последовательности.

Такое представление функции $F$ позволяет провести аналогию между восстановлением функции $F$ и биоинформационной задачей сборки генома. Способ саморегуляции сетевой инфраструктуры промышленных объектов при воздействии угроз безопасности реализует перенос и адаптацию принципов сборки генома на сетевые инфраструктуры промышленных объектов с использованием математического аппарата графов де Брёйна, обеспечивая повышение скорости их реконфигурации.

Из представления фиг. 1 следует, что функция $f_i$ может быть выполнена либо одиночным устройством, являющимся в терминах графовой модели вершиной $v_i$, либо одиночным устройством $v_t$, либо путем взаимодействия устройств (в терминах графовой модели – маршрутом на графе): $(v_t, v_u, v_r)$. Функция $f_j$ может быть выполнена либо устройством $v_j$, либо устройствами ($v_q, v_e$), либо устройствами $(v_h, v_l, v_y)$.

Сопоставление каждой из функций, входящей в состав целевой, множества вариантов ее реализации целесообразно по следующим причинам. Ее легко выполнить на этапе подготовки промышленного объекта к работе в небезопасной среде – кластеризация выполняется крайне быстро. Время поиска в кластере во много раз меньше, чем поиск с полным перебором вершин в графе. К тому же, в условиях примерно одинакового размера всех кластеров, эффективен будет параллельный поиск (в случае, если нарушение безопасности затронуло несколько звеньев цепочки целевой функции). Представление функции промышленного объекта в виде графов де Брёйна обеспечивает связывание кластеров, и именно за счет них обеспечивается получение более сложных функций, каждая из которых выполняется множеством устройств.

Если с использованием кластера для нарушенной функции $f_j$ был получен альтернативный вариант ее реализации, необходимо учесть, что до нее выполнялась, например, функция $f_i$, а после $f_j$ будет выполнена $f_k$. В таких условиях необходимо, чтобы все узлы сетевой инфраструктуры промышленного объекта, реализующие эти функции, могли взаимодействовать между собой. При этом, поскольку время на поиск, выбор и применение сценария саморегуляции сильно ограничен временем реализации угрозы безопасности, выбирают такие устройства для восстановления функции $f_j$, которые позволят организовать более быстрое взаимодействие с устройствами из кластеров других функций.

Вершины графа де Брёйна – строки фиксированной длины, и они соединены ребром тогда, когда суффикс первой строки является префиксом второй строки. Для применения данного графа к промышленному объекту концевой вершине каждого подграфа рассматриваемого кластера сопоставляют метку – список, с какими вершинами она может взаимодействовать. И при выборе способа восстановления функции ориентируются на те вершины, с которых начинается выполнение функции из соседнего кластера.

Если между вершинами $v_i$ и $v_j$ была нарушена связь, вследствие чего не была выполнена функция $f_j$, то в кластере для функции $f_j$ находят альтернативные пути ее

реализации. Важным условием является выбор такого маршрута, при котором устройства из разных кластеров смогут взаимодействовать, и время выполнения нового маршрута будет минимальным.

Пусть каждая вершина характеризуется тремя символами (обозначениями вершин): первый символ обозначает вершину, которая начинает выполнять функцию, второй символ – вершину, которая заканчивает выполнение функции, третий символ – вершину не из кластера, с которой смежна рассматриваемая вершина. Если вершина обозначена двумя символами – значит, рассматриваемая функция выполняется одним устройством (тем же, что стоит на первом месте в наименовании вершины).

Использование графа де Брёйна позволяет быстро выполнять отбор подходящего сценария саморегуляции. Общая схема осуществления саморегуляции сетевой инфраструктуры промышленного объекта представлена на фиг. 2. Саморегуляцию сетевой инфраструктуры промышленных объектов реализуют следующим образом:

1. Выполняют определение последовательностей функций, для которых требуется восстановить маршрут. Каждая из последовательностей начинается с функции, которая может быть реализована без восстановления маршрута. Исключение составляет случай, когда требуется полное восстановление маршрута всей целевой функции.

2. Для каждой последовательности $f_{i1} \dots f_{ik}$:

2.1. Построение вспомогательного графа осуществляют по следующим правилам:

каждый слой графа отвечает за выполнение одной из функций в последовательности $f_{i1} \dots f_{ik}$;

слои в графе размещены в том же порядке, что и соответствующие им функции в последовательности;

каждый слой $j$ включает множество вершин и последовательностей вершин, принадлежащих кластеру, соответствующему функции $f_{ij}$;

между всеми соседними слоями кроме первого и второго строят ребра по принципу построения ребер в графе де Брёйна.

2.2. Из всех вершин и последовательностей вершин первого слоя выбирают ту вершину или последовательность вершин, которая реализует функцию $f_{i1}$ в текущем состоянии маршрута. Обозначают данную вершину (или, в случае выбора последовательности, последнюю вершину в последовательности) как $w$. Далее создают ребра между вершиной $w$ и некоторыми вершинами второго слоя: между одиночными вершинами, которые в графе являются соседями $w$, и между вершинами, которые являются соседями $w$ в исходном графе и с которых начинается последовательность вершин. В том случае, когда требуется восстановить маршрут всей целевой функции, ребра между всеми слоями строят по принципу построения ребер в графе де Брейна, первый и второй слои не являются исключением.

На данном шаге также создают два пустых множества: $A$ – множество вершин, достижимых из первого слоя; $D$ – множество вершин, ведущих к тупиковым путям.

2.3. До тех пор, пока не будет найден маршрут или пока не окажется, что подходящих маршрутов нет, осуществляют следующие действия:

2.3.1. Выполняют поиск путей, соединяющих первый и последний слои.

1) Помечают множество достижимых вершин (с привязкой к слою, в котором они находятся), используя поиск в глубину или в ширину, начинающийся из вершины $w$. Если какая-либо из вершин последнего слоя помечается, то маршрут найден. Переходят к следующей последовательности.

2) Выбирают наиболее длинный путь, начинающийся из первого слоя и не содержащий в себе тупиковых вершин или последовательностей вершин. Длину пути измеряют количеством слоев, через которые данный путь проходит.

3) Обозначают последнюю вершину в этом пути как $t$. Соединяют вершину $t$ с вершиной следующего слоя, если эта одиночная вершина, которая в графе является соседней с $t$ и не принадлежит множеству тупиковых вершин; или с этой вершины начинается последовательность вершин, не являющейся тупиковой, и эта вершина является соседней с вершиной $t$ в исходном графе.

4) Если вершину не удается соединить ни с одной из вершин следующего слоя, вершина переносится из множества достижимых вершин в множество тупиковых.

5) Выполняют возврат к шагу 1), помечая множество достижимых вершин.

2.3.2. Если путь не был найден, слева к графу добавляют еще один слой, соответствующий функции, предшествующей текущей рассматриваемой последовательности функций. Нумерацию слоев сдвигают (первый становится вторым и т.д.). По принципу, указанному на шаге 2.2, выбирают новую вершину $w$, строят ребра между первым и вторым слоями графа, строят дополнительные ребра между вторым и третьим слоем. При этом не строят ребра между остальными слоями, поскольку они уже построены ранее. Если новый слой добавить невозможно (это происходит, когда на предыдущем шаге уже был добавлен слой), соответствующий началу целевой функции, то далее действия не осуществляют, так как без внесения дополнительных модификаций в исходный граф восстановить маршрут нельзя.

3. Объединяют обнаруженные маршруты.

На фиг. 3 представлен пример графа, моделирующего подсистему анализа энергетического промышленного объекта. Точечными стрелками представлена целевая функция $F = f_7\left(f_6\left(f_5\left(f_4\left(f_3(f_2(f_1))\right)\right)\right)\right)$. В результате воздействия угрозы безопасности, заключающейся в выведении из строя трех компонентов ($v_{10}, v_{12}, v_{13}$), выполнена саморегуляция с использованием графа, представленного на фиг. 4. Новое графовое представление и новый маршрут реализации целевой функции представлены на фиг. 5.

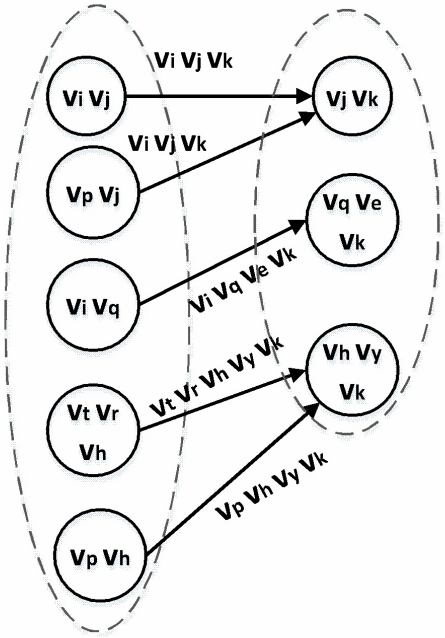
В итоге для любого типа угрозы безопасности при первом ее проявлении в сети инициируется саморегуляция сетевой инфраструктуры промышленных объектов при воздействии угроз безопасности. За счет сохраненного графового представления целевой функции, сформированных кластеров для каждой функции и сохраненных графов де Брёйна для связей между кластерами быстро находится решение, позволяющее восстановить нарушенную функцию, входящую в состав целевой функции. Способ позволяет перестроить инфраструктуру сети быстрее, чем развивается нарушение

безопасности, и за счет этого повысить безопасность и устойчивость промышленных объектов.

## (57) Формула изобретения

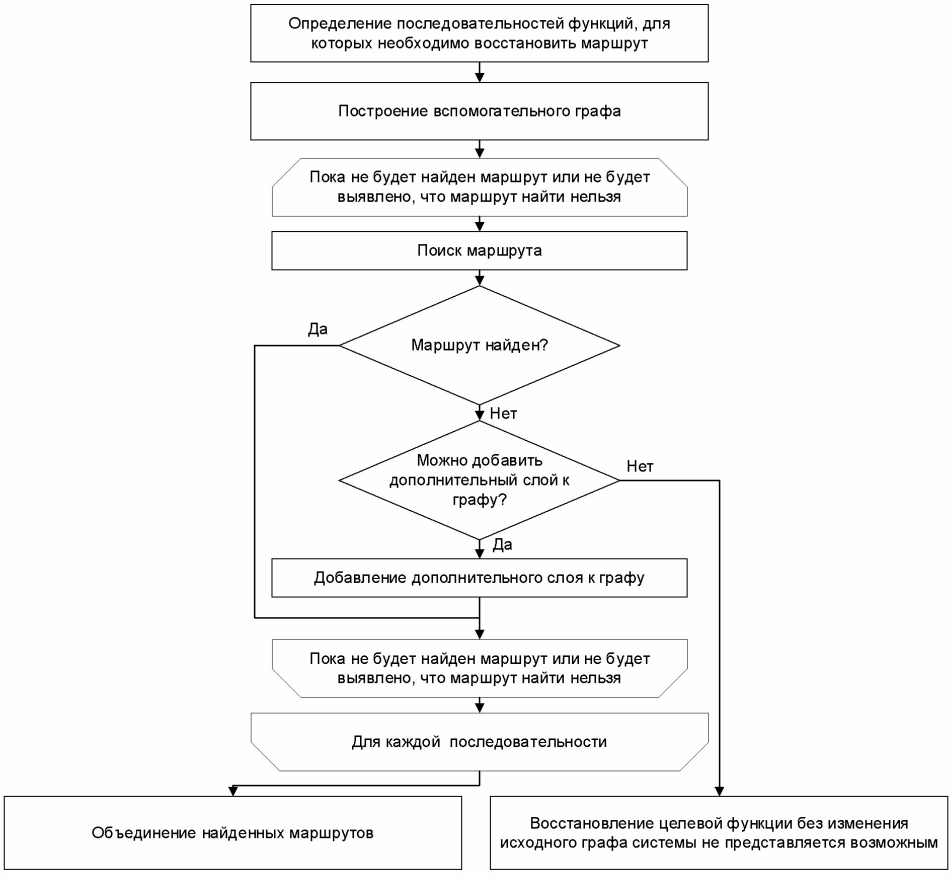
Способ саморегуляции сетевой инфраструктуры промышленных объектов при воздействии угроз безопасности, включающий перестроение сети при получении сигнала от модуля или системы обнаружения угроз безопасности, расположенных на отдельном компьютере, отличающийся тем, что для сетевой инфраструктуры промышленного объекта заранее формируют и сохраняют в базы данных, расположенные на сервере баз данных, набор функциональных последовательностей, характеризующий целевую функцию промышленного объекта, графовое представление сетевой инфраструктуры промышленного объекта, наборы связей и операций между кластерами каждой функции из набора функциональных последовательностей, полученные с использованием графов де Брёйна, многоуровневый граф, представляющий все возможные варианты реализации целевой функции, затем при получении сигнала от модуля или системы обнаружения угроз безопасности, расположенных на отдельном компьютере, о том, какой узел графа затронут сетевой атакой, составляют список нарушенных функций из набора функциональных последовательностей, выполняют поиск по сохраненным в базах данных кластерам функций, наборам связей и операций между кластерами, многоуровневому графу вариантов перестроения сетевой структуры, затем выбирают наиболее быстрый для применения вариант перестроения сетевой структуры и применяют к текущей структуре сети, затем выполняют проверку того, что целевая функция снова выполняется узлами сетевой инфраструктуры.

1


Vi Vj
Vi Vj Vk
Vj Vk
Vi Vj Vk
Vp Vj
Vq Ve
Vk
Vi Vq
Vi Vq Ve Vk
Vh Vy
Vk
Vt Vr Vh Vy Vk
Vt Vr
Vh
Vp Vh Vy Vk
Vp Vh

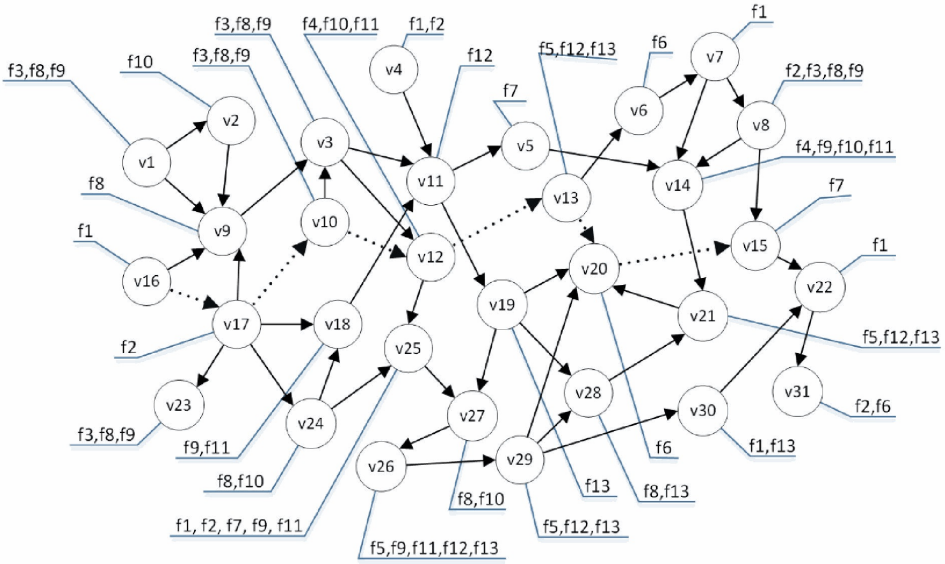
Фиг. 1

2


Определение последовательностей функций, для которых необходимо восстановить маршрут
Построение вспомогательного графа
Пока не будет найден маршрут или не будет выявлено, что маршрут найти нельзя
Поиск маршрута
Маршрут найден?
Да
Нет
Можно добавить дополнительный слой к графу?
Нет
Да
Добавление дополнительного слоя к графу
Пока не будет найден маршрут или не будет выявлено, что маршрут найти нельзя
Для каждой последовательности
Объединение найденных маршрутов
Восстановление целевой функции без изменения исходного графа системы не представляется возможным

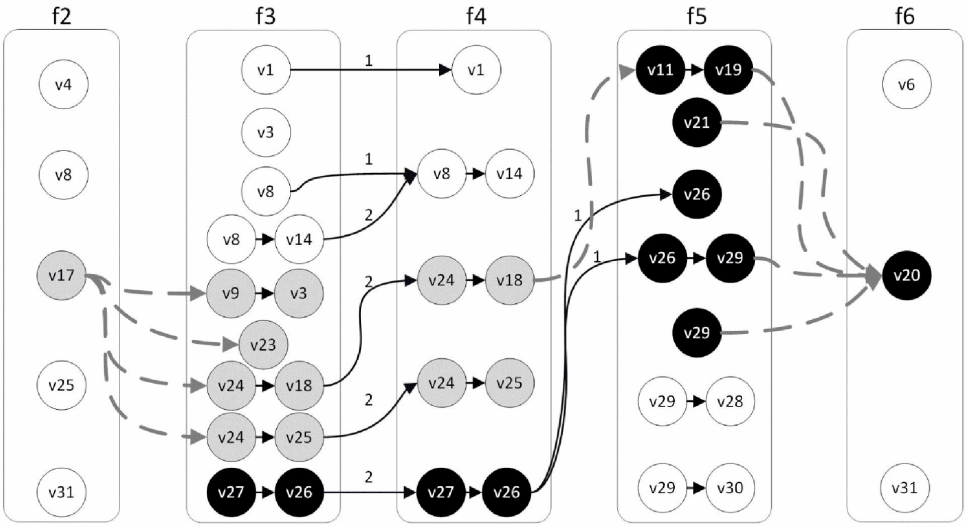
Фиг. 2

3

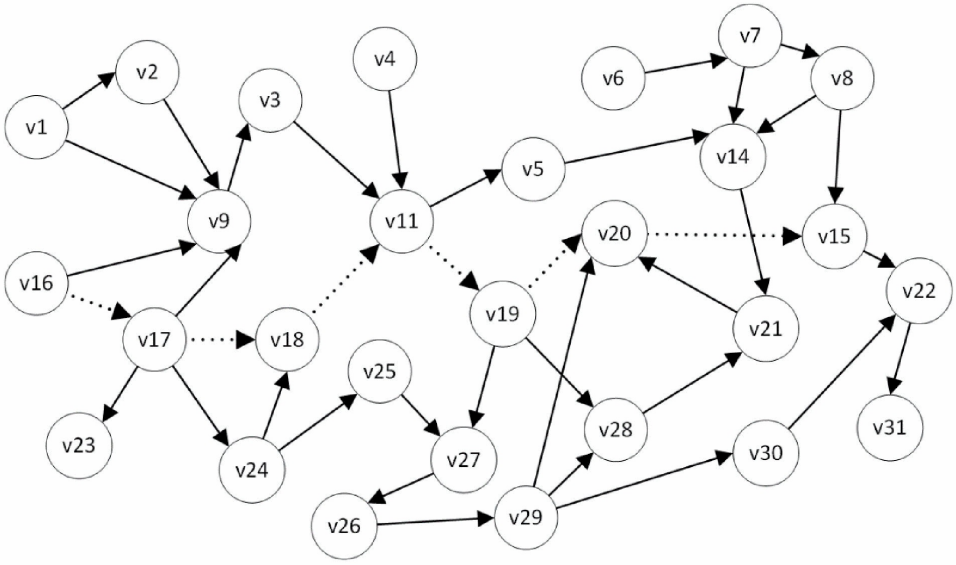

f3,f8,f9
f10
f3,f8,f9
f4,f10,f11
f1,f2
f12
f5,f12,f13
f6
f1
f2,f3,f8,f9
f7
f4,f9,f10,f11
f8
f7
f1
f1
f2
f5,f12,f13
f3,f8,f9
f9,f11
f8,f10
f1, f2, f7, f9, f11
f5,f9,f11,f12,f13
f8,f10
f13
f8,f13
f5,f12,f13
f6
f1,f13
f2,f6
v1
v2
v3
v4
v5
v6
v7
v8
v9
v10
v11
v12
v13
v14
v15
v16
v17
v18
v19
v20
v21
v22
v23
v24
v25
v26
v27
v28
v29
v30
v31

Фиг. 3

4


f2
f3
f4
f5
f6
v4
v8
v17
v25
v31
v1
v3
v8
v8
v14
v9
v3
v23
v24
v18
v24
v25
v27
v26
v1
v8
v14
v24
v18
v24
v25
v27
v26
v11
v19
v21
v26
v26
v29
v29
v29
v28
v29
v30
v6
v20
v31
1
1
2
2
2
2
1
1

Фиг. 4


v1
v2
v3
v4
v5
v6
v7
v8
v9
v11
v14
v15
v16
v17
v18
v19
v20
v21
v22
v23
v24
v25
v26
v27
v28
v29
v30
v31

Фиг. 5