(19) Евразийское патентное ведомство

(11) 039497 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.02.03

(21) Номер заявки
201992834

(22) Дата подачи заявки
2019.12.25

(51) Int. Cl. ***G06F 21/56*** (2013.01)
H04L 29/06 (2006.01)
G06F 7/08 (2006.01)

(54) СПОСОБ ОЦЕНКИ УСТОЙЧИВОСТИ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ К КОМПЬЮТЕРНЫМ АТАКАМ

(31) **2019109130**
(32) **2019.03.28**
(33) **RU**
(43) **2020.09.30**

(71)(73) Заявитель и патентовладелец:
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО" (ФГАОУ ВО "СПбПУ") (RU)

(72) Изобретатель:
Зегжда Дмитрий Петрович, Лаврова Дарья Сергеевна, Павленко Евгений Юрьевич (RU)

(74) Представитель:
Кадиев И.Г. (RU)

(56) US-A1-20180159890
US-A1-20170126712
US-A1-20170289187
AU-B2-2017221858
US-A1-20180159881

(57) Изобретение относится к области компьютерных систем, а именно к киберфизическим системам и оценке их устойчивости к компьютерным атакам. Технической проблемой заявляемого изобретения является разработка способа оценки устойчивости КФС к компьютерным атакам с целью оценки степени сопротивляемости системы деструктивным информационным воздействиям со стороны злоумышленника. Технический результат заключается в увеличении степени защищенности киберфизической системы от компьютерных атак за счет оценки ее устойчивости к компьютерным атакам в различные моменты времени и контроля значений полученных оценок, направленного на поддержание значения устойчивости системы в определенных пределах, гарантирующих способность системы сохранять способность корректного функционирования даже в условиях компьютерных атак.

039497 B1

039497 B1

Изобретение относится к области компьютерных систем, а именно, к киберфизическим системам (КФС) и оценке их устойчивости к компьютерным атакам.

Известен способ численной оценки устойчивости промышленных систем управления (патент США №US20130132149A1, опубл. 10.06.2010) и решающий задачу получения количественной оценки устойчивости промышленных систем управления, учитывая нежелательные инциденты, связанные с промышленной системой управления. Рассматриваются нежелательные инциденты, результатом которых является возможность операторов системы выполнять ненадлежащие операции.

Способ направлен на расширение понятия устойчивости, определяя устойчивость как способность и скорость восстановления нормальной работы системы после нежелательного инцидента [0008].

Способ базируется на оценке рисков и реализует циклический процесс, включающий этапы: определения набора критических нежелательных инцидентов, выполнения оценки риска для этих инцидентов (с точки зрения частоты их возникновения и финансовых затрат для системы), определения действий для минимизации частоты каждого нежелательного инцидента, минимизации времени, необходимого для восстановления производительности промышленной системы управления до ее первоначального уровня производительности.

Данное изобретение обладает следующими недостатками:

1. Авторы определяют устойчивость как скорость восстановления промышленной системы управления после того, как произошел нежелательный инцидент [0008]. Это говорит о том, что данный способ реализует апостериорную защиту системы от атак, в условиях того, что нарушение работоспособности системы, вызванное кибератакой, уже произошло. Такой подход не позволяет сохранить работоспособность системы, а только восстановить ее. В связи с этим, данное изобретение неприменимо в промышленных системах управления критическими технологическими процессами (ядерная энергетика, военная отрасль и т.д.). Успешная реализация атак на такие системы может привести к катастрофическим последствиям, поэтому приоритетной задачей является задача сопротивления системы к кибератакам, которая не решается данным изобретением.

2. Критерием устойчивости данного изобретения является производительность промышленной системы управления, что неэффективно при реализации злоумышленником низкоинтенсивных кибератак, а также целенаправленных (Advanced Persistent Threat) кибератак, целью которых может являться не выведение промышленной системы из строя, а изменение логики и параметров ее функционирования с сохранением производительности.

Известны способ и система (патент США №US9203859B2, опубл. 01.02.2012) для моделирования киберфизической безопасности, симуляции и архитектуры для интеллектуальных энергосетей (Smart Grid). Способ используется для оценки по меньшей мере одной угрозы безопасности для сложных систем. Каждая угроза определяется как кибератака или физическая атака на цель, целью может являться как кибер-компонент, так и физический компонент системы. Согласно пп.3, 4 CLAIMS, оценка включает в себя оценку серьезности угрозы кибератаки на один или несколько физических компонентов.

В данном способе оценка формируется на основании наличия хотя бы одной уязвимости в компонентах системы. Серьезность угрозы оценивается на основании созданного отчета об угрозе (п.9 CLAIMS). В связи с этим можно сделать вывод о том, что оценка может быть получена только в случае найденной уязвимости. При этом, в описании к изобретению отмечается, что термин "угроза" связан с вызовом катастрофы или с ухудшением производительности. Отсюда следует, что изобретение обладает следующими недостатками:

1) оценка не инвариантна к типу компьютерных атак и может быть вычислена только в случае реализации злоумышленником на систему атак определенного типа;

2) оценка может быть получена только в отдельных случаях - когда обнаружена уязвимость, и для атак определенного типа, что неэффективно.

Известны способ и система обеспечения киберустойчивости (патент США №US20180103052A1, опубл. 11.10.2016), основывающиеся на извлечении данных, выявлении событий, оценке и ранжировании уведомлений безопасности, оценке риска и формировании рекомендаций по его снижению.

Процесс извлечения знаний включает в себя автоматический сбор информации о поведении каждой сущности. Полученная информация используется для создания графа знаний [0007]. Для обнаружения и локализации аномалий в поведении сущностей используются предварительно обученные искусственные нейронные сети [0011]. При обнаружении аномалии производится построение цепочки состояний, которая связывала бы текущее состояние с небезопасным состоянием. При обнаружении цепочки состояний с высокой вероятностью, данная цепочка передается эксперту для изменения конфигурации системы [0017].

Сбор информации о поведении системы включает сбор трафика и сбор информации из логов. Поскольку не учитываются показатели устройств, отследить аномалию в показателях физического процесса, осуществляемого в киберфизической системе, не представляется возможным.

Для оценки вероятности перехода системы в небезопасное состояние должна иметь место аномалия. При осуществлении ряда компьютерных атак время между появлением аномалий в системе и завершением атаки может быть незначительным. Таким образом, метод может не успеть обнаружить атаку

до ее завершения. В том случае, когда метод позволит обнаружить факт атаки до момента ее завершения, метод сможет ее прервать. Однако в таком случае атака может успеть оказать деструктивное воздействие на систему.

Отсюда следует, что изобретение обладает следующими недостатками:

1) не учитывает показатели, характеризующие физические процессы, протекающие в системе, что негативно влияет на точность обнаружения компьютерных атак, поскольку некоторые атаки могут быть реализованы через уязвимости в прошивке или программном обеспечении физических устройств;

2) изобретение реализует апостериорный подход к защите от компьютерных атак, поскольку оценка киберустойчивости может быть получена только в случае обнаружения аномалии. Таким образом, не обеспечивается противодействие компьютерным атакам, проводимым на систему.

Известен способ моделирования атак на киберфизические системы (патент США № US 20180159890A1, опубл. 07.06.2018), обеспечивающий:

получение данных динамической модели, относящихся к компонентам состояния графа, представляющего киберфизическую систему;

генерацию соответствующего значения метрики уязвимости для каждой из множества связей между соответствующим набором исходных узлов графа и соответствующим набором целевых узлов графа;

определение множества таких узлов графа, для которых метрика уязвимости превышает заданный порог.

Изобретение обладает следующими недостатками:

1. В заявляемом изобретении оценивается устойчивость системы к атакам, в то время как в указанном аналоге оцениваются метрики уязвимости системы к атакам (абзац [0005]). Эти два термина отличаются друг от друга: метрики уязвимости характеризуют подверженность системы к воздействию, метрики устойчивости - способность системы работать даже в неблагоприятных для нее условиях (таких, как, например, выход из строя некоторых узлов).

2. В изобретении используется динамическая модель системы в виде графа (абзацы [0005], [0021], [0022] и т.д.), в то время как в заявляемом изобретении система моделируется статическим графом, на котором в дальнейшем ищутся различные маршруты (пути). Использование динамического графа порождает большие вычислительные затраты при оценке метрик уязвимости, поскольку значения каждый раз, при малейшем изменении, должны вычисляться заново, с учетом добавленных/удаленных связей между узлами.

3. В изобретении отсутствуют (в частности, в указанных абзацах [0002], [0005], [0021], пунктах формулы 1, 11 и рисунках 1, 3, 4) сведения о поиске альтернативных маршрутов на графе и формировании их множества; о вычислении мощности множества альтернативных маршрутов. Это подчеркивает различную направленность рассматриваемого аналога и заявляемого изобретения.

4. Из пункта [0025] формулы указанного аналога видно, что для оценки метрик используется предсказательная модель (формулы (1) и (2)), в отличие от метрики, вычисляемой в заявляемом изобретении, которая базируется только на оценке мощности множества альтернативных маршрутов на графе. Метрика на основе предсказательной модели требует накопления статистических данных и вычисления корреляционных коэффициентов, что более трудоемко и менее точно, чем получение с заданной периодичностью единственного числа, характеризующего значение метрики мощности множества альтернативных маршрутов.

Таким образом, рассмотренное изобретение не решает задач, которые решает заявляемое изобретение, поскольку оно направлено на оценку метрик уязвимости отдельных узлов киберфизических систем, а не на оценку киберустойчивости всей киберфизической системы в целом. Кроме того, математический аппарат, используемый в рассматриваемом аналоге, является более трудоемким с точки зрения вычислений, чем математический аппарат заявляемого изобретения.

Технической проблемой заявляемого изобретения является разработка способа оценки устойчивости КФС к компьютерным атакам с целью оценки степени сопротивляемости системы деструктивным информационным воздействиям со стороны злоумышленника.

Технический результат заключается в увеличении степени защищенности киберфизической системы от компьютерных атак за счет оценки ее устойчивости к компьютерным атакам в различные моменты времени и контроля значений полученных оценок, направленного на поддержание значения устойчивости системы в определенных пределах, гарантирующих способность системы сохранять способность корректного функционирования даже в условиях компьютерных атак.

Технический результат достигается способом оценки устойчивости киберфизических систем к компьютерным атакам, который включает компьютерное представление киберфизической системы в виде графа, определение критически важных процессов для киберфизической системы с использованием технической документации и компьютерное представление выделенных критически важных процессов в виде маршрутов на графе, моделирующем киберфизическую систему, в предлагаемом способе в базе данных, располагающейся на сервере баз данных, формируется список правил работы КФС, содержащий описание соотношений между процессами системы с использованием логических предикатов, описывающих одновременное выполнение процессов, запрет на одновременное выполнение процессов, ини-

циирование выполнения процесса, и описание условий для поиска альтернативных маршрутов на графе, затем список правил записывается в базу данных, располагающуюся на сервере баз данных, затем для всех процессов КФС назначаются весовые коэффициенты, представляющие собой вещественное число в промежутке от 0 до 1, при этом, выделенным критически важным процессам назначаются минимальные весовые коэффициенты, затем значения коэффициентов для каждого процесса записываются в базу данных, затем для каждого процесса КФС, представленного как маршрут на графе, в этом же графе ищутся альтернативные маршруты, с учетом ограничений, описанных в списке правил работы КФС, затем найденные для каждого процесса альтернативные маршруты формируют множества альтернативных маршрутов, для каждого множества вычисляется его мощность, представляющая собой число элементов в множестве, затем вычисляется оценка устойчивости киберфизической системы к компьютерным атакам путем вычисления суммы произведений числа альтернативных маршрутов для маршрута, отражающего каждый процесс КФС, на весовой коэффициент соответствующего процесса, затем значение вычисленной оценки сохраняется в базу данных как "эталонное", также в базу данных записываются значения концов диапазона, характеризующего корректное функционирование КФС, вычисляемые как отклонения в меньшую и большую сторону для "эталонного" значения, затем в различные моменты времени снова производится оценка устойчивости и выполняется контроль значений полученных оценок, заключающийся в сравнении полученных значений с "эталонным" значением или с диапазоном значений, затем, если новое значение оценки не попадает в диапазон, выполняется его запись в отдельную таблицу базы данных, содержащую аномальные значений оценки устойчивости, затем на экран компьютера выводится уведомление о том, что устойчивость КФС снизилась в результате возможной компьютерной атаки на КФС, что является сигналом об автоматическом внесении изменений в структуру КФС для поддержания значения устойчивости системы в определенных пределах, описываемых диапазоном значений, содержащим отклонения от "эталонного" значения оценки.

Т.е. решение поставленной задачи обеспечивается тем, что в способе оценки устойчивости КФС к компьютерным атакам реализуется представление КФС в виде графа, а процессов, выполняемых системой - в виде маршрутов на графах. Для каждого процесса (маршрута на графе) определяется множество маршрутов, аналогичных ему по функциям, обеспечивающих выполнение того же процесса, только с использованием других компонентов КФС. Сумма произведений числа альтернативных маршрутов для маршрута, отражающего каждый процесс КФС, на весовой коэффициент соответствующего процесса, и является численной оценкой устойчивости КФС к компьютерным атакам.

Увеличение степени защищенности КФС от компьютерных атак напрямую связано с оценкой устойчивости КФС к компьютерным атакам за счет того, что контроль значений оценок, которые могут быть получены в любое время, позволит по отклонениям значений оценок от "эталонного" зафиксировать компьютерную атаку, реализуемую на КФС, на ранней стадии. Это связано с высокой чувствительностью разработанной оценки устойчивости к изменениям в системе.

Изобретение поясняется чертежом, изображающим схему работы способа.

Важность получения численного значения оценки устойчивости системы к компьютерным атакам обоснована тем, что контроль данного значения позволит обнаружить попытки реализации атаки на систему на ранней стадии и тем самым даст возможность администратору безопасности предотвратить компьютерную атаку, сохранив способность КФС к корректной работе.

Важность решения данной задачи связана также с тем, что большинство КФС интегрированы с промышленными областями деятельности, в том числе, критическими (энергетика, транспорт, военная отрасль и т.д.), поэтому успешная реализация компьютерных атак на такие системы может повлечь за собой катастрофические последствия.

Требования к оценке устойчивости:

1. Оценка должна быть инвариантна к типу компьютерных атак. Данное свойство означает, что оценка не должна учитывать сложность, ресурсоёмкость и другие параметры атаки, она должна быть независима от них. Для оценки важен сам факт проведения компьютерной атаки и возможность нарушения безопасности работы КФС.

2. Оценка должна быть универсальной. Данное свойство означает, что оценка применима для КФС различных типов.

3. Оценка должна быть количественной. КФС имеют сложную структуру, в их состав входит большое число различных компонент, каждый из которых может быть подвержен деструктивному воздействию. В связи с этим, качественной характеристики безопасности КФС, позволяющий ответить на вопрос "Находится ли КФС в состоянии безопасности?" положительно или отрицательно, недостаточно. Для обеспечения защищенности КФС необходимо знать о возможных способностях КФС противодействовать деструктивным воздействиям.

4. Оценка должна быть вычислима в режиме реального времени. Данное требование обосновано необходимостью своевременного обнаружения атак и реагирования на них.

5. Оценка должна быть сравнимой. Это означает, что должна быть возможность сравнивать полученные значения оценок и ранжировать их, сравнивая безопасность различных КФС или уровень безопасности одной и той же КФС в различные моменты времени.

Предлагается трактовать безопасность КФС как сохранение устойчивости в условиях компьютерных атак на ее компоненты. Определение устойчивости КФС состоит в оценке возможности нахождения ее в устойчивом состоянии, причем данная оценка должна проводиться для системы в целом, а не отдельных ее элементов.

Для получения численной оценки устойчивости, киберфизическая система представляется в виде ориентированного графа G=<V,E>, где:

1) все компоненты системы формируют множество вершин графа V, V={$\nu_1,\nu_2,...\nu_n$}. При этом, каждая вершина ν_i характеризуется кортежем <id,type,Ф,NPr>, id - идентификатор устройства, type- тип устройства (датчик, актуатор, контроллер, интеллектуальное устройство и т.п.).

$\Phi_{v_i} = \{\varphi^m_{v_{i_1}}, \varphi^m_{v_{i_2}}, \cdots, \varphi^m_{v_{i_k}}\}$ - множество функции, реализуемых вершиной ν_i, где верхний индекс m∈{0; 1} обозначает режим выполнения функции (использует ли компонент ν_i функциональность $\varphi_{v_{ij}}$ в текущем процессе КФС или нет. NPr - число процессов, в которых задействован данный компонент;

2) все потоки информации между компонентами КФС формируют множество дуг E,E={$e_1,e_2,...e_l$}. Исходящая из вершины дуга означает, что данная вершина (компонент КФС) осуществляет управляющее информационное воздействие на другую вершину (другой компонент КФС).

С использованием документации на КФС и/или с помощью экспертных знаний для КФС определяется множество процессов Proc, которые она должна реализовывать, Proc=($proc_1,proc_2,...proc_p$}. Каждый процесс $proc_i$ характеризуется кортежем <id,R,Ф',Weight>:

1) id - идентификатор процесса;

2) R={S_{ij}}- множество маршрутов графа G, элементы которого представляют собой совокупность различных путей из вершины ν_i в вершину ν_j:

$$S_{ij} = \{s_{ij}^{(1)}, s_{ij}^{(2)}, ...\}, \quad s_{ij}^{(k)} = < v_i, ..., v_j >, \quad k = 1, ..., |S_{ij}|.$$

3) Множество Ф' - множество функций, которые должны быть выполнены в рамках данного процесса, в определенной очередности, $\Phi' = (\varphi^{(1)}_{v_{i_p}}, \varphi^{(2)}_{v_{i_t}}, \ldots, \varphi^{(N)}_{v_{i_a}})$. При выполнении маршрута S_{ij} на графе происходит переход между вершинами графа, характеризующийся поочередным выполнением функций $\varphi^{(1)}_{v_{i_p}}, \varphi^{(2)}_{v_{i_t}}, \ldots, \varphi^{(N)}_{v_{i_a}}$, где N - число функций, задействованных в маршруте S_{ij}, а p,t,a - индексы задействованных функций соответствующих вершин.

4) Weight - весовой коэффициент, Weights ∈ (0;1], означающий критичность данного процесса для данной КФС - чем процесс критичнее, тем ближе значение Weight к 0.

Между процессами КФС, описываемыми множеством Proc, устанавливаются соотношения. Каждый процесс по отношению к другому/другим может быть независимым (протекание процесса не зависит от выполнения процессов) или зависимым (протекание процесса зависит от выполнения процессов). Для зависимых процессов могут быть следующие соотношения:

1) процессы выполняются одновременно;

2) процессы никогда не выполняются одновременно;

3) процесс является следствием непустого множества других процессов;

4) процесс инициирует выполнение непустого множества других процессов.

Установленные соотношения описываются в виде правил с использованием логических предикатов и записываются в базу данных.

Каждому процессу КФС из множества Proc автоматически назначаются значения Weight. При этом, должно быть выполнено следующее условие: если некоторое множество процессов Proc',Proc' ∈ Proc, инициирует процесс $proc_i$, значение $Weight_{proc_i}$ которого близко к 0, каждому процессу из множества Proc' должен быть назначен такой же весовой коэффициент, как $Weight_{proc_i}$.

Описываются правила выбора альтернативных по функциям маршрутов на графе. Альтернативным по функциям считается маршрут, в рамках которого обеспечивается выполнение такой же совокупности функций в такой же очередности. Множество альтернативных маршрутов обозначим AltR{S'_{ij}}, $s_{ij}: \varphi_{s_{ij}} = \varphi_{v_i} + \cdots + \varphi_{v_j}$. Тогда $s'_{ij} = s_{ij} \Leftrightarrow \varphi_{s_{ij}} = \varphi_{s'_{ij}}$.

При этом, альтернативный маршрут может включать в себя большее число вершин, чем исходный маршрут. Однако для этого должны выполняться следующие условия:

1) вершина графа ν_i может быть заменена вершиной ν_k, если $type_{v_i} = type_{v_k}$;

2) вершина графа ν_i, реализующая функции $\varphi_{v_{ij}}$, может быть заменена множеством вершин ($\nu_t,\nu_u,...,\nu_z$), если совокупно они реализуют суперпозицию функций $\varphi_{v_{i_i}} = \varphi_{v_t} * \varphi_{v_u} \cdots \varphi_{v_z}$;

3) вершина графа ν_i может быть включена в альтернативный маршрут только в том случае, если число процессов, в которых она будет задействована, не превышает NPr - число процессов, в которых

задействован данный компонент.

Оценка устойчивости КФС к компьютерным атакам связана с количеством альтернативных маршрутов, характеризующих каждый процесс, реализуемый КФС.

Для каждого процесса $proc_i \in Proc$ выполняется поиск альтернативных маршрутов, для чего для каждого маршрута $s_{kj} \in R_{proc_i}$ выполняется поиск S'_{kj}, формирующих множество S'_{kj}. Для каждого множества S'_{kj} вычисляется его мощность $|S'_{kj}|$.

Значениям мощностей для каждого процесса $proc_i$ сопоставляется весовой коэффициент $Weight_{proc_i}$, соответствующий данному процессу. Итоговая формула оценки, обозначаемой $Eval_G$, вычисляется по следующей формуле:

$$Eval_G = \left|S'_{proc_1}\right| \cdot Weight_{proc_1} + \left|S'_{proc_2}\right| \cdot Weight_{proc_2} + \cdots + \left|S'_{proc_p}\right| \cdot$$
$$Weight_{proc_1} = \sum_{i=1}^{p} |S'_{proc_i}| \cdot Weight_{proc_i}$$

За счет того, что у всех маршрутов на графе, отражающих выполнение наиболее критичных процессов КФС, будет маленький вес, даже незначительное изменение числа маршрутов для критичных процессов приведет к большему изменению численного значения оценки, чем изменение числа некритичных маршрутов.

Способ предполагает:

1. Представление КФС в виде ориентированного графа, где компоненты системы - вершины графа, а информационный обмен между компонентами - дуги.

2. Определение множества процессов, необходимых для работы КФС.

3. Определение соотношений между процессами:

1) процессы выполняются одновременно;

2) процессы никогда не выполняются одновременно;

3) процесс является следствием непустого множества других процессов;

4) процесс инициирует выполнение непустого множества других процессов.

4. Описание соотношений между процессами с помощью логики предикатов и их запись в базу данных правил работы КФС.

5. Назначение весовых коэффициентов каждому процессу таким образом, что значение коэффициента принадлежит промежутку (0;1], и значения коэффициентов наиболее критичных процессов близки к 0.

6. Описание правил выбора альтернативных по функциям маршрутов на графе, отражающих следующие условия выбора маршрутов:

1) замена вершин графа может быть выполнена только в том случае, если эти вершины характеризуют устройства КФС одного типа;

2) одна вершина может быть заменена на несколько вершин, если совокупно это множество вершин реализует в нужной последовательности набор функций, выполняемых изначальной вершиной;

3) вершина графа может быть включена в альтернативный маршрут только в том случае, если число процессов, в которых она будет задействована, не превышает число процессов, в которых задействован данный компонент.

7. Формирование для каждого процесса множества альтернативных маршрутов на графе.

8. Вычисление мощности множества альтернативных маршрутов.

9. Вычисление оценки устойчивости КФС к компьютерным атакам как суммы произведений числа альтернативных маршрутов для маршрута, отражающего каждый процесс КФС, на весовой коэффициент соответствующего процесса.

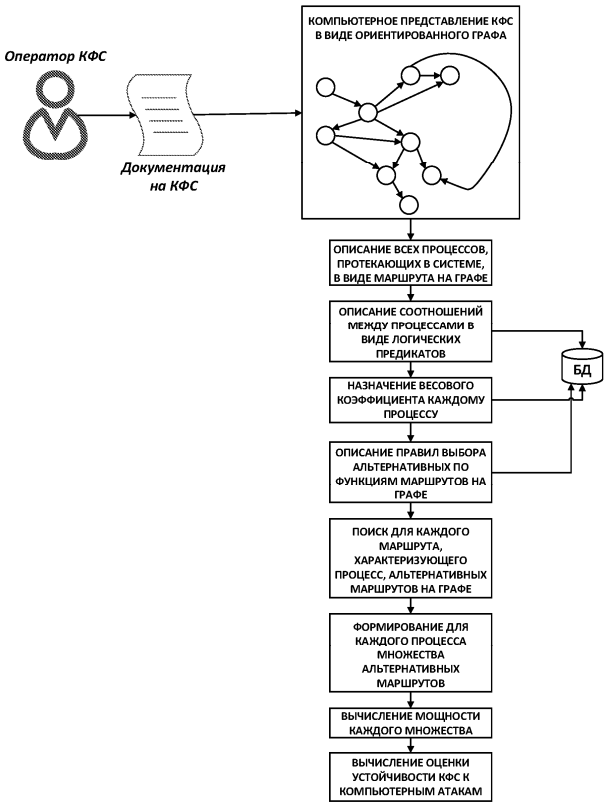
В итоге для КФС вычисляется оценка устойчивости, которая может быть получена в любой момент времени для всей системы в целом. При этом, она чувствительна к изменениям в системе, относящимся к наиболее важным ее процессам.

Данный способ обеспечивает повышение точности обнаружения компьютерных атак за счет возможности получения значений оценок в различные моменты времени и сравнения полученных значений с "эталонным" значением или с диапазоном значений для корректно функционирующей КФС, находящейся в состоянии безопасности. Высокая чувствительность значения оценки, предлагаемой к вычислению в данном изобретении, к изменениям в параметрах протекания критических для данной КФС процессов, также увеличивает точность обнаружения компьютерных атак на систему. Оценка инвариантна к типу деструктивных воздействий, что, в совокупности с рассмотренными ранее особенностями, обеспечивает увеличение степени защищенности киберфизической системы от компьютерных атак.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Способ оценки устойчивости киберфизических систем (КФС) к компьютерным атакам, включающий компьютерное представление КФС в виде графа, определение критически важных процессов для КФС с использованием технической документации и компьютерное представление выделенных критически важных процессов в виде маршрутов на графе, моделирующем КФС, и отличающийся тем, что в

базе данных, располагающейся на сервере баз данных, формируется список правил работы КФС, содержащий описание соотношений между процессами системы с использованием логических предикатов, описывающих одновременное выполнение процессов, запрет на одновременное выполнение процессов, инициирование выполнения процесса и описание условий для поиска альтернативных маршрутов на графе, затем список правил записывается в базу данных, располагающуюся на сервере баз данных, затем для всех процессов КФС назначаются весовые коэффициенты, представляющие собой вещественное число в промежутке от 0 до 1, при этом выделенным критически важным процессам назначаются минимальные весовые коэффициенты, затем значения коэффициентов для каждого процесса записываются в базу данных, затем для каждого процесса КФС, представленного как маршрут на графе, в этом же графе ищутся альтернативные маршруты с учетом ограничений, описанных в списке правил работы КФС, затем найденные для каждого процесса альтернативные маршруты формируют множества альтернативных маршрутов, для каждого множества вычисляется его мощность, представляющая собой число элементов в множестве, затем вычисляется оценка устойчивости киберфизической системы к компьютерным атакам путем вычисления суммы произведений числа альтернативных маршрутов для маршрута, отражающего каждый процесс КФС, на весовой коэффициент соответствующего процесса, затем значение вычисленной оценки сохраняется в базу данных как эталонное, также в базу данных записываются значения концов диапазона, характеризующего корректное функционирование КФС, вычисляемые как отклонения в меньшую и большую сторону для эталонного значения, затем в различные моменты времени снова производится оценка устойчивости и выполняется контроль значений полученных оценок, заключающийся в сравнении полученных значений с эталонным значением или с диапазоном значений, затем, если новое значение оценки не попадает в диапазон, выполняется его запись в отдельную таблицу базы данных, содержащую аномальные значений оценки устойчивости, затем на экран компьютера выводится уведомление о том, что устойчивость КФС снизилась в результате возможной компьютерной атаки на КФС, что является сигналом об автоматическом внесении изменений в структуру КФС для поддержания значения устойчивости системы в определенных пределах, описываемых диапазоном значений, содержащим отклонения от эталонного значения оценки.



Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2