РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 663 473**(13) **C1**

(51) МПК
H04L 29/06 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 29/06 *(2018.05);* ***H04L 29/06911*** *(2018.05);* ***H04L 29/06884*** *(2018.05);* ***H04L 63/0227*** *(2018.05);* ***H04L 63/1425*** *(2018.05);* ***H04L 63/1441*** *(2018.05)*

(21)(22) Заявка: **2017132568, 18.09.2017**

(24) Дата начала отсчета срока действия патента:
18.09.2017

Дата регистрации:
06.08.2018

Приоритет(ы):
(22) Дата подачи заявки: **18.09.2017**

(45) Опубликовано: **06.08.2018** Бюл. № **22**

Адрес для переписки:
302034, г. Орел, ул. Приборостроительная, 35, Академия ФСО России, ОНТИ

(72) Автор(ы):
Закалкин Павел Владимирович (RU),
Добрышин Михаил Михайлович (RU),
Стародубцев Юрий Иванович (RU),
Гуцын Руслан Викторович (RU),
Карайчев Сергей Юрьевич (RU)

(73) Патентообладатель(и):
Федеральное государственное казенное военное образовательное учреждение высшего образования "Академия Федеральной службы охраны Российской Федерации" (Академия ФСО России) (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2480937 C2, 27.04.2013. RU 2405184 C1, 27.11.2010. RU 2355024 C2, 10.05.2009. US 2004/0250124 A1, 09.12.2004. US 2014/0283030 A1, 18.09.2014.**

(54) СПОСОБ ЗАЩИТЫ ОТ ПРОВОДИМЫХ ОДНОВРЕМЕННО КОМПЬЮТЕРНЫХ АТАК

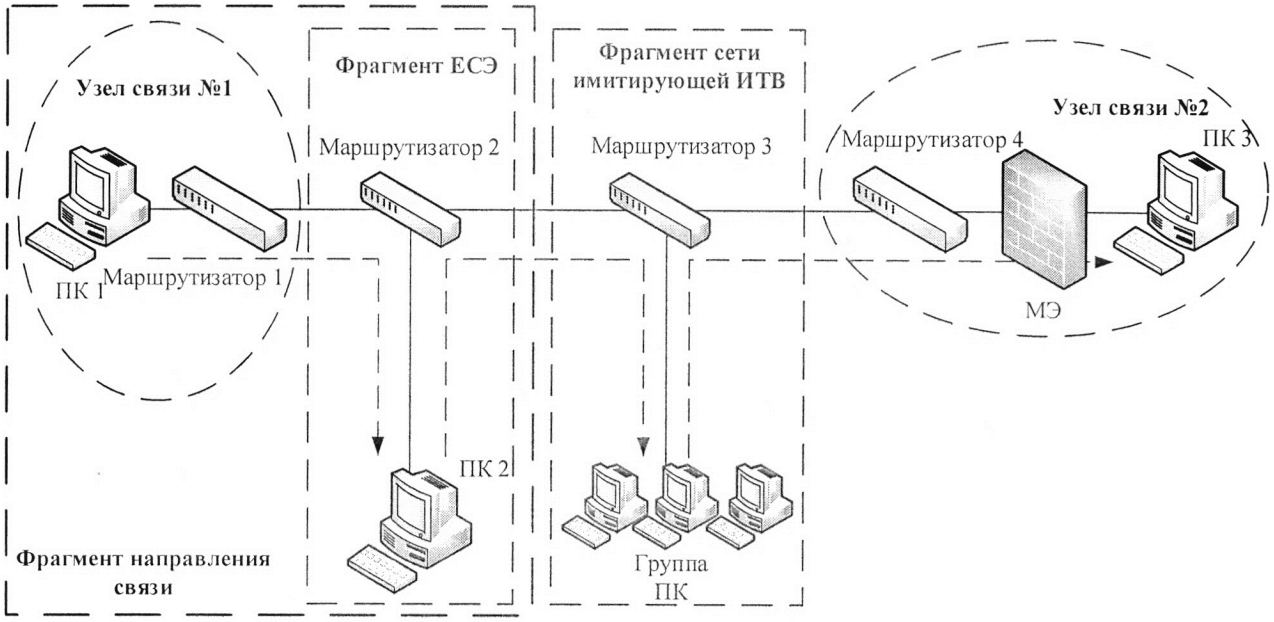
(57) Реферат:

Изобретение относится к области вычислительной техники. Техническим результатом является повышение достоверности идентификации информационно-технических воздействий за счет анализа параметров различных видов информационно-технических воздействий, которые поступают как одиночно, так и несколько совместно, что позволяет определять их совокупность. Способ защиты от проводимых совместно компьютерных атак заключается в том, что обрабатывают на сенсорах все запросы к сервису с дальнейшим агрегированием полученной информации, обновляют правила фильтрации на коллекторах, используя полученную от сенсоров информацию, фильтруют трафик на центрах очистки по заданным правилам фильтрации, при этом формируют структуру узла связи, формируют направление связи и фрагмент внешней сети, генерирующий информационно-технические воздействия, затем формируют множество информационно-технических воздействий, после ввода заданных правил фильтрации имитируют поступление информационно-технических воздействий на узел сети связи, при этом постепенно увеличивают их интенсивность от минимального количества к максимальному, измеряют и запоминают значения интенсивности воздействия, при которой система защиты информации начинает реагировать на информационно-технические воздействия, и далее в процессе имитации поступления информационно-технических воздействий формируют множество правил фильтрации, которые соответствуют определенным информационно-техническим воздействиям,

RU 2663473 C1

RU 2663473 C1

вводят полученное множество правил фильтрации в реальную систему, затем фильтруют трафик на центрах очистки, используя правила, скорректированные по множеству правил фильтрации. 2 ил.



Фиг.2

RU 2663473 C1

RU 2663473 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 663 473**(13) **C1**

(51) Int. Cl.
H04L 29/06 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 29/06 *(2018.05);* ***H04L 29/06911*** *(2018.05);* ***H04L 29/06884*** *(2018.05);* ***H04L 63/0227*** *(2018.05);* ***H04L 63/1425*** *(2018.05);* ***H04L 63/1441*** *(2018.05)*

(21)(22) Application: **2017132568, 18.09.2017**

(24) Effective date for property rights:
18.09.2017

Registration date:
06.08.2018

Priority:
(22) Date of filing: **18.09.2017**

(45) Date of publication: **06.08.2018** Bull. № **22**

Mail address:
302034, g. Orel, ul. Priborostroitelnaya, 35, Akademiya FSO Rossii, ONTI

(72) Inventor(s):
Zakalkin Pavel Vladimirovich (RU),
Dobryshin Mikhail Mikhajlovich (RU),
Starodubtsev Yurij Ivanovich (RU),
Gutsyn Ruslan Viktorovich (RU),
Karajchev Sergej Yurevich (RU)

(73) Proprietor(s):
Federalnoe gosudarstvennoe kazennoe voennoe obrazovatelnoe uchrezhdenie vysshego obrazovaniya "Akademiya Federalnoj sluzhby okhrany Rossijskoj Federatsii" (Akademiya FSO Rossii) (RU)

(54) METHOD OF PROTECTION FROM SIMULTANEOUSLY COMPUTER ATTACKS

(57) Abstract:

FIELD: computer equipment.

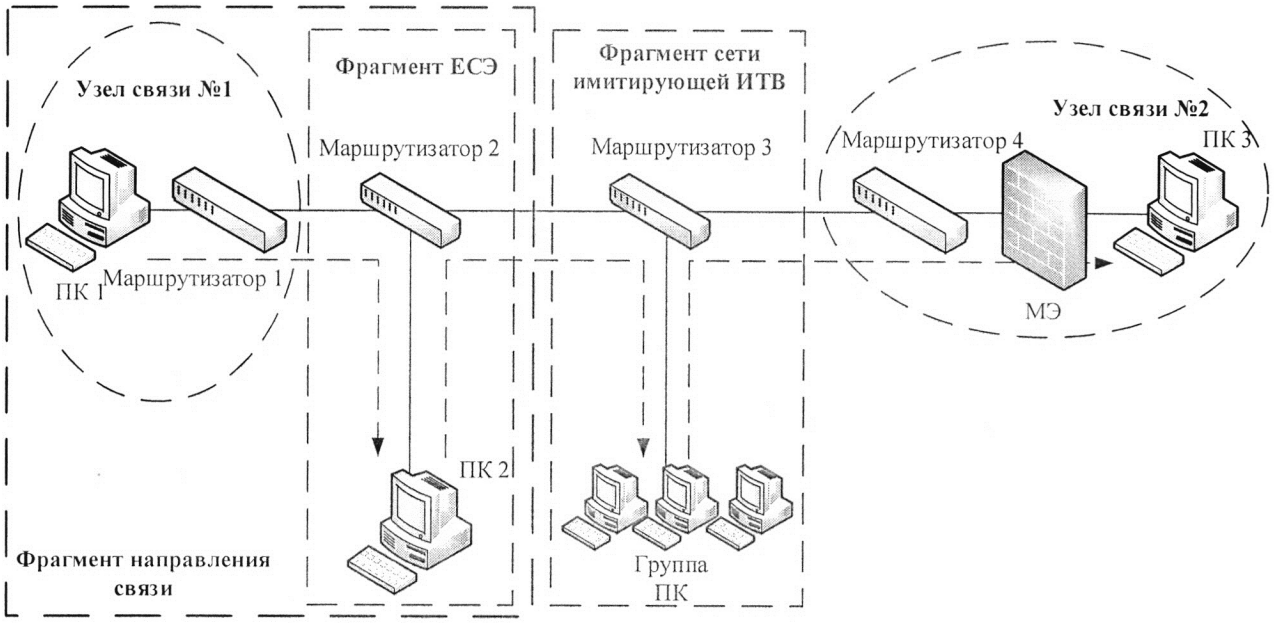
SUBSTANCE: invention relates to computer equipment. Way to protect against co-operative computer attacks is to process all the requests to the service on the sensors with further aggregation of the information received, update the filtering rules on the collectors, using the information received from the sensors, filter traffic on the cleaning centers according to the specified filtering rules, while forming the structure of the communication center, forming the direction of communication and the fragment of the external network that generates information and technical effects, then form a set of information and technical impacts, after entering the specified filtering rules, imitate the arrival of information and technical impacts on the network node, while gradually increasing their intensity from the minimum amount to the maximum, measure and store the values of the intensity of the impact, at which the information protection system begins to respond to information and technology impacts, and further in the process of imitation of the inflow of information and technical influences form a set of filtration rules that correspond to certain information and technical influences, enter the resulting set of filtering rules into the real system, then filter traffic on the cleaning centers, using rules, corrected according to the set of filtering rules.

EFFECT: technical result is increased reliability of the identification of information and technical impacts due to the analysis of the parameters of various types of information and technical impacts, which come both singly and somewhat together, which allows us to determine their totality.

1 cl, 2 dwg

RU 2663473 C1

RU 2663473 C1



Фиг.2

RU 2663473 C1

RU 2663473 C1

Изобретение относится к области вычислительной техники и может использоваться для обнаружения информационно-технических воздействий как одиночных, так и проводимых совместно.

Толкование используемых терминов:

информационно-телекоммуникационная сеть связи - совокупность информационно-вычислительных систем, объединенных системой передачи данных [Центр стратегических оценок и прогнозов. Информационная война и защита информации. Словарь основных терминов и определений, www.csef.ru, Москва, 2011, стр. 25].

В качестве элементов сети связи рассматриваются узлы и каналы (линии) связи [Ермишян А.Г., Теоретические основы построения систем военной связи в объединениях и соединениях: Учебник. Часть 1. Методологические основы построения организационно-технических систем военной связи. СПб.: ВАС, 2005. 740 с.].

Под информационно-техническими воздействиями понимается применение способов и средств информационного воздействия на информационно-технические объекты, на технику и вооружение в интересах достижения поставленных целей [Центр стратегических оценок и прогнозов. Информационная война и защита информации. Словарь основных терминов и определений www.csef.ru Москва, 2011, стр. 25].

Известен «Способ обеспечения устойчивого функционирования системы связи» (патент RU №2405184, G05B 23/00, G06F 17/50, опубл. 27.11.2010 г., Бюллетень №33), заключающийся в том, что систему связи разворачивают в рабочее состояние, фиксируют дестабилизирующие воздействия на ее структурные элементы, формируют имитационную модель сети связи, моделируют процесса функционирования системы связи при воздействиях, проводят упреждающую реконфигурацию функционирующей системы связи.

Недостатком данного способа является низкая достоверность идентификации информационно-технических воздействий, обусловленная отсутствием фиксации и определения двух и более совместно возникающих информационно-технических воздействий на узле связи.

Известен «Способ мониторинга безопасности автоматизированных систем» (патент РФ №2355024, G06F 15/00, G06F 17/00, опубл. 10.05.2009 г. Бюллетень №13). Способ заключается в том, что для мониторинга безопасности автоматизированных систем предварительно задают множество контролируемых параметров, характеризующих безопасность автоматизированной системы, и их эталонных значений. Затем выполняют цикл измерений значений контролируемых параметров и сравнения их с эталонными значениями, при их несовпадении формируют сигнал тревоги о выходе контролируемых параметров в группе за пределы допустимых значений, после чего блокируют работу элементов автоматизированной системы и формируют отчет о состоянии автоматизированной системы.

Недостатком данного способа является низкая достоверность идентификации информационно-технических воздействий, обусловленная отсутствием фиксации и определения двух и более совместно возникающих информационно-технических воздействий на узле связи.

Наиболее близким по технической сущности и выполняемым функциям аналогом (прототипом) к заявленному является система и способ уменьшения ложных срабатываний при определении сетевой атаки (патент РФ №2480937, H04L 29/06, G06F 15/16, G06F 21/30, опубл. 27.04.2013 г. Бюлл. №12), заключающийся в том, что перенаправляют трафик к сервису на сенсоры и центры очистки, обрабатывают на сенсорах все запросы к сервису с дальнейшим агрегированием полученной информации,

обновляют правила фильтрации на коллекторах, используя полученную от сенсоров информацию, корректируют обновленные правила фильтрации с помощью управляющего модуля на основании статистики предыдущих сетевых атак, фильтруют трафик на центрах очистки, используя заданные правила фильтрации, при этом центры очистки подключены к магистральным каналам связи по каналам с высокой пропускной способностью.

Недостатком способа-прототипа является низкая достоверность идентификации информационно-технических воздействий, обусловленная отсутствием фиксации и определения двух и более совместно возникающих информационно-технических воздействий на узле связи.

Задачей изобретения является создание способа защиты от проводимых совместно компьютерных атак. Техническим результатом изобретения является повышение достоверности идентификации информационно-технических воздействий за счет анализа параметров различных видов информационно-технических воздействий, которые поступают как одиночно, так и несколько совместно, что позволяет определять их совокупность.

Задача изобретения решается тем, что в способе защиты от проводимых совместно компьютерных атак выполняется следующая последовательность действий.

Обрабатывают на сенсорах все запросы к сервису с дальнейшим агрегированием полученной информации, обновляют правила фильтрации на коллекторах, используя полученную от сенсоров информацию, фильтруют трафик на центрах очистки, по заданным правилам фильтрации.

Согласно изобретению дополнительно формируют структуру узла связи, формируют направление связи и фрагмент внешней сети, генерирующий информационно-технические воздействия, затем формируют множество информационно-технических воздействий. После ввода заданных правил фильтрации имитируют поступление информационно-технических воздействий на узел сети связи, при этом постепенно увеличивают их интенсивность от минимального количества к максимальному. Измеряют и запоминают значения интенсивности воздействия, при которой система защиты информации начинает реагировать на информационно-технические воздействия, и далее в процессе имитации поступления информационно-технических воздействий формируют множество правил фильтрации, которые соответствуют определенным информационно-техническим воздействиям. Вводят полученное множество правил фильтрации в реальную систему. Затем фильтруют трафик на центрах очистки, используя правила, скорректированные по множеству правил фильтрации.

Результаты поиска известных решений в данной и смежной областях техники с целью выявления признаков, совпадающих с отличительными от прототипов признаками заявленного изобретения, показали, что они не следуют явным образом из уровня техники. Из определенного заявителем уровня техники не выявлена известность влияния предусматриваемых существенными признаками заявленного изобретения на достижение указанного технического результата. Следовательно, заявленное изобретение соответствует условию патентоспособности "изобретательский уровень".

Заявленный способ поясняется чертежами, на которых показаны:

фиг. 1 - блок-схема способа защиты от проводимых совместно компьютерных атак;

фиг. 2 - схема реализации способа защиты от проводимых совместно компьютерных атак.

Заявленный способ поясняется блок-схемой способа защиты от проводимых совместно компьютерных атак (фиг. 1), где в блоке 1 осуществляют задание исходных

данных. Исходными данными являются:

- счетчик k=1 - количество совместно имитируемых ИТВ;

- n - количество заданных ИТВ.

В блоке 2 формируют узел связи включающий сетевое оборудование и систему защиты информации (СЗИ) (фиг. 2) [Климов С.М., Сычев М.П. и др. Экспериментальная оценка противодействия компьютерным атакам на стендовом полигоне. Электронное учебное издание / Москва.: ФГБОУ ВО «Московский государственный технический университет им. Н.Э. Баумана», 2013. - 114 с.].

В качестве узла связи №2 будем понимать персональный компьютер оконечного пользователя (ПК 3, фиг. 2) и коммутационное оборудование, подключенное к нему (маршрутизатор 4, фиг. 2) [процесс настройки маршрутизатора: Базовая настройка маршрутизатора Использование Cisco Configuration Professional. Электронный ресурс: http://www.cisco.com/cisco/web/support/RU/108/1089/1089854_basic-router-config-ccp-00.pdf]. В качестве СЗИ используется межсетевой экран (МЭ, фиг. 2) [процесс настройки межсетевого экрана: Киберсейф межсетевой экран для Windows. Руководство пользователя http://cybersafesoft.com/cs-firewall.pdf].

В блоке 3 создают направление связи и фрагмент внешней сети моделирующей ИТВ.

В качестве направления связи понимается узел связи и фрагмента Единой сети электросвязи (ЕСЭ) (фиг. 2).

В качестве фрагмента ЕСЭ будем понимать коммутационное оборудование (маршрутизатор 2, фиг. 2) имитирующее ЕСЭ [процесс настройки маршрутизатора: Базовая настройка маршрутизатора Использование Cisco Configuration Professional. Электронный ресурс: http://www.cisco.com/cisco/web/support/RU/108/1089/1089854_basic-router-config-ccp-00.pdf] и управляемое персональным компьютером (ПК 2, фиг. 2).

В качестве фрагмента внешней сети понимается botnet сеть, имитирующая ИТВ и состоящая из коммутационного оборудования (маршрутизатор 3, фиг. 2) [процесс настройки маршрутизатора: Базовая настройка маршрутизатора Использование Cisco Configuration Professional. Электронный ресурс: http://www.cisco.com/cisco/web/support/RU/108/1089/1089854_basic-router-config-ccp-00.pdf] и подключенную к нему группу ПК (фиг. 2) осуществляющую имитацию ИТВ на узел связи №2.

В блоке 4 формируют множество ИТВ.

При формировании данного множества учитывают множество современных ИТВ, например такие воздействия как:

1) отказ в обслуживании [Котенко И.В., Уланов А.В. Многоагентное моделирование распределенных атак «отказ в обслуживании» и механизмов защиты от них / Труды СПИИРАН т. 1, №3 2006 г.];

2) атака посредника или атака «человек по середине» (англ. Man in the middle (MITM)) [Варламов О.О. "О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры" Известия ТРТУ / Тематический выпуск // №7 / том 62 / 2006 г. С. 218];

3) сканирование портов [Различные приемы сканирования портов https://nmap.org/man/ru/man-port-scanning-techniques.html; 7 онлайн сканеров для поиска открытых портов на сервере https://habrahabr.ru/company/hosting-cafe/blog/281943/1;

4) SQL - инъекции [SQL-инъекции http://www.cyberguru.ru/database/sql/sql-injections.html?showall=1; SQL injection для начинающих. Часть 1 https://habrahabr.ru/post/148151/1.

В блоке 5 водят заданные правила фильтрации. Формируют начальные правила, используемые в реальной СЗИ (МЭ), сформированные и заданные, как в способе-

прототипе.

В блоке 6 имитируют поступление ИТВ на узел связи.

На первоначальном этапе осуществляется последовательная имитация единичных ИТВ на узел связи. Затем осуществляется совместная имитация ИТВ в количестве k (во всех возможных комбинациях) до достижения счетчиком k значения k>n.

В блоке 7 все ИТВ начинаются с минимального значения интенсивности воздействия, затем интенсивность ИТВ постепенно увеличивается от минимального количества к максимальному. При достижении интенсивности воздействия, при которой СЗИ начинает реагировать на ИТВ, в блоке 8 фиксируют и сохраняют полученные значения интенсивности ИТВ.

В блоке 9 осуществляют проверку количества совместно имитируемых ИТВ. В случае совместной имитации нескольких ИТВ переходят к блоку 11, в противном случае переходят к блоку 10 и формируют правила фильтрации для ИТВ, имитируемого в данный момент. После чего переходят к блоку 6 и имитируют поступление следующего ИТВ на узел связи.

В блоке 11 Рассчитывают количество всех возможных комбинаций ИТВ совместно воздействующих на узел связи. При этом количество комбинаций будет изменяться в зависимости от количества совместно воздействующих ИТВ на узел связи. Расчет всех возможных комбинаций при заданном количестве ИТВ является известной задачей и представлен в [Н.Я. Виленкин «Комбинаторика», М.: Наука. Гл. ред. физ. - мат. лит., 1969. - 323 с.]

$$C_n^m = \frac{n!}{m!(n-m)!}$$

другими словами находится сочетание из n элементов по m.

В блоке 12 формируют правила фильтрации для имитируемых в текущий момент времени ИТВ.

В блоке 13 счетчик k увеличивают на единицу и переходят к блоку 14, где осуществляется проверка выполнения условия k>n. В случае выполнения условия переходят к блоку 15, в противном случае переходят к блоку 6 и имитируют совместное поступление ИТВ на узел связи в количестве равном значению счетчика k.

В блоке 15 на основе сформированных правил фильтрации при имитации одиночных и нескольких ИТВ проводимых совместно, формируют множество правил фильтрации, которые в блоке 16 дополнительно вводятся в реально функционирующую систему.

В блоке 17 на сенсорах осуществляют обработку всех запросов к сервису с дальнейшим агрегированием полученной информации.

В блоке 18 осуществляют фильтрацию трафика, используя заданные правила.

Расчет эффективности заявленного способа проводился согласно коэффициента несоответствия Тэйла осуществлялась оценка точности прогноза выполненного по построенной модели [Е.Ю. Пискунов «Модификация коэффициента Тэйла». Электронный журнал «Известия Иркутской государственной экономической академии» №5, 2012 г.].

$$\upsilon = \frac{\sqrt{\sum (P_t - A_t)^2}}{\sqrt{\sum A_t^2}}$$

где P_t и A_t - соответственно предсказанное и фактическое (реализованное) изменение переменной. Коэффициент $\upsilon=0$, когда все $P_t=A_t$ (случай совершенного прогнозирования);

υ=1, когда процесс прогнозирования приводит к той же среднеквадратической ошибке, что и «наивная» экстраполяция неизменности приростов; υ>1, когда прогноз дает худшие результаты, чем предположение о неизменности исследуемого явления.

Достоинством коэффициента Тэйла является возможность использования при сопоставлении качества прогнозов, получаемых на основе различных методов и моделей.

Способ-прототип предполагает одновременное воздействие одного вида ИТВ, таким образом, предсказанные значения будут соответствовать фактическим только в этом случае и значение коэффициента υ будет меньше единицы и стремиться к нулю. Однако при совместном воздействии нескольких ИТВ предсказанные значения не будут соответствовать фактическим значениям и значение коэффициента υ будет превышать единицу, что говорит о высокой степени неточности выполненного прогноза.

В предлагаемом способе проводится совместная имитация нескольких видов ИТВ, что позволяет повысить степень соответствия предсказанных значений фактическим. Таким образом, в отличие от способа-прототипа в предлагаемом способе значение коэффициента υ будет меньше единицы и стремиться к нулю в случае как одиночных, так и совместных множественных воздействии ИТВ.

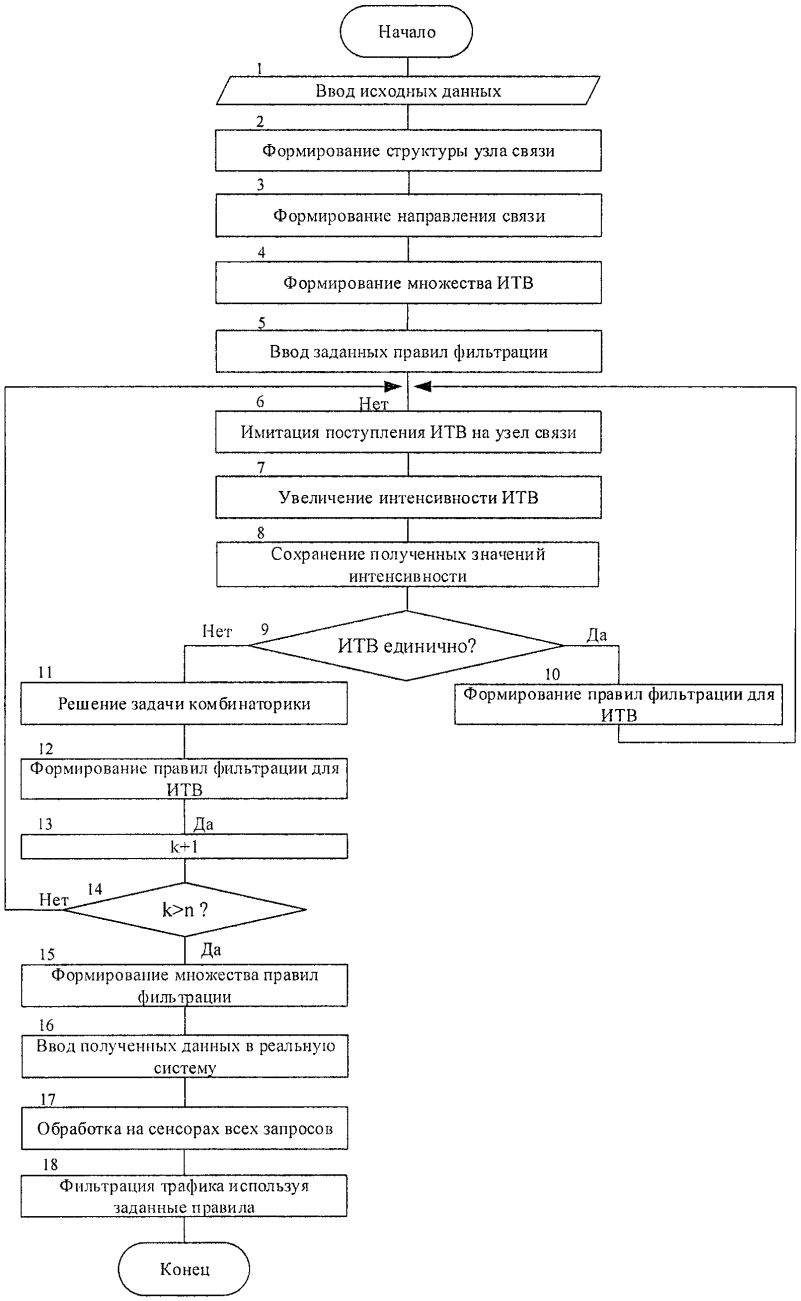
На основании этого следует вывод, что заявленный способ защиты от проводимых совместно компьютерных атак повышает достоверность идентификации информационно-технических воздействий за счет анализа параметров различных видов информационно-технических воздействий, которые поступают как одиночно, так и несколько совместно, что позволяет определять их совокупность.

(57) Формула изобретения

Способ защиты от проводимых совместно компьютерных атак заключается в том, что обрабатывают на сенсорах все запросы к сервису с дальнейшим агрегированием полученной информации, обновляют правила фильтрации на коллекторах, используя полученную от сенсоров информацию, фильтруют трафик на центрах очистки по заданным правилам фильтрации, отличающийся тем, что формируют структуру узла связи, формируют направление связи и фрагмент внешней сети, генерирующий информационно-технические воздействия, затем формируют множество информационно-технических воздействий, после ввода заданных правил фильтрации имитируют поступление информационно-технических воздействий на узел сети связи, при этом постепенно увеличивают их интенсивность от минимального количества к максимальному, измеряют и запоминают значения интенсивности воздействия, при которой система защиты информации начинает реагировать на информационно-технические воздействия, и далее в процессе имитации поступления информационно-технических воздействий формируют множество правил фильтрации, которые соответствуют определенным информационно-техническим воздействиям, вводят полученное множество правил фильтрации в реальную систему, затем фильтруют трафик на центрах очистки, используя правила, скорректированные по множеству правил фильтрации.

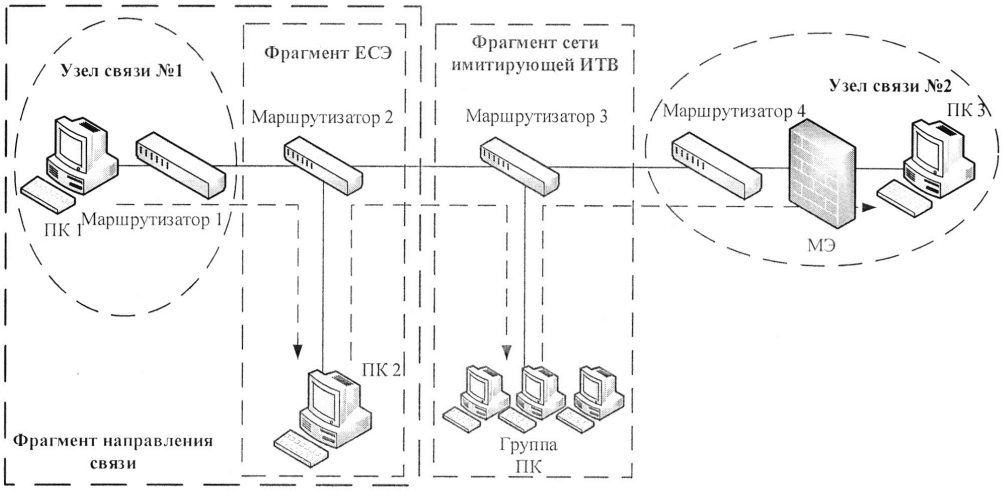
1

1


Начало
1
Ввод исходных данных
2
Формирование структуры узла связи
3
Формирование направления связи
4
Формирование множества ИТВ
5
Ввод заданных правил фильтрации
6
Нет
Имитация поступления ИТВ на узел связи
7
Увеличение интенсивности ИТВ
8
Сохранение полученных значений интенсивности
Нет
9
ИТВ единично?
Да
11
Решение задачи комбинаторики
10
Формирование правил фильтрации для ИТВ
12
Формирование правил фильтрации для ИТВ
13
Да
k+1
Нет
14
k>n ?
Да
15
Формирование множества правил фильтрации
16
Ввод полученных данных в реальную систему
17
Обработка на сенсорах всех запросов
18
Фильтрация трафика используя заданные правила
Конец

Фиг.1

2


Узел связи №1
Фрагмент ЕСЭ
Фрагмент сети имитирующей ИТВ
Узел связи №2
Маршрутизатор 2
Маршрутизатор 3
Маршрутизатор 4
ПК 3
ПК 1
Маршрутизатор 1
МЭ
ПК 2
Группа ПК
Фрагмент направления связи

Фиг.2