РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2016 136 226**(13) **A**

(51) МПК
G06F 21/54 (2013.01)

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2016136226, 08.09.2016**

Приоритет(ы):
(22) Дата подачи заявки: **08.09.2016**

(43) Дата публикации заявки: **15.03.2018** Бюл. № **08**

Адрес для переписки:
125212, Москва, Ленинградское ш., 39а, стр. 3, АО "Лаборатория Касперского", Управление по интеллектуальной собственности, Надежда Васильевна Кащенко

(71) Заявитель(и):
Акционерное общество "Лаборатория Касперского" (RU)

(72) Автор(ы):
Купреев Олег Викторович (RU),
Гальченко Антон Борисович (RU),
Устинов Михаил Валерьевич (RU),
Кондратов Виталий Викторович (RU),
Кусков Владимир Анатольевич (RU)

(54) **Способы обнаружения аномальных элементов веб-страниц**

(57) Формула изобретения

1. Способ обнаружения аномального элемента веб-страницы на основании статистической модели веб-страницы, в котором:

а) строят статистическую модель веб-страницы, где:

- получают по меньшей мере одним веб-клиентом, реализованным на компьютерном устройстве пользователя, веб-страницу от веб-сервера, при этом веб-страница содержит скрипт, который при выполнении собирает сведения о содержимом по меньшей мере одного элемента веб-страницы на стороне веб-клиента и оправляет собранные сведения с компьютерного устройства пользователя серверу управления;

- выполняют вышеуказанный скрипт с помощью веб-клиента, который собирает сведения о содержимом по меньшей мере одного элемента веб-страницы на стороне веб-клиента и отправляет собранные сведения с компьютерного устройства пользователя серверу управления;

- преобразуют с помощью сервера управления полученные сведения в по меньшей мере один N-мерный вектор, где N-мерный вектор характеризует содержимое по меньшей мере одного элемента веб-страницы;

- создают с помощью сервера управления статистическую модель веб-страницы, которая представляет собой по крайней мере один кластер в N-мерном пространстве, при этом кластер содержит по крайней мере один N-мерный вектор;

б) обнаруживают аномальный элемент веб-страницы на основании построенной статистической модели веб-страницы, где:

- получают по меньшей мере одним веб-клиентом, реализованным на компьютерном устройстве пользователя, веб-страницу от веб-сервера, при этом веб-страница содержит скрипт, который при выполнении собирает сведения о содержимом по меньшей мере одного элемента веб-страницы на стороне веб-клиента и оправляет собранные сведения с компьютерного устройства пользователя серверу управления;

RU 2016136226 A

RU 2016136226 A

- выполняют вышеуказанный скрипт с помощью веб-клиента, который собирает сведения о содержимом по меньшей мере одного элемента веб-страницы на стороне веб-клиента и отправляет собранные сведения с компьютерного устройства пользователя серверу управления;

- преобразуют с помощью сервера управления полученные сведения в по меньшей мере один N-мерный вектор, где N-мерный вектор характеризует содержимое по меньшей мере одного элемента веб-страницы;

- сравнивают с помощью сервера управления полученный N-мерный вектор с кластерами статистической модели веб-страницы, где определяют расстояние между полученным N-мерным вектором элемента и центрами всех кластеров статистической модели;

- обнаруживают с помощью сервера управления в результате сравнения аномальный элемент веб-страницы, где аномальным признается элемент, когда выполняется по крайней мере одно из следующих условий:

● расстояние между полученным N-мерным вектором и центрами всех кластеров статистической модели в N-мерном пространстве больше радиусов этих кластеров;

● мера близости между полученным N-мерным вектором и центрами всех кластеров модели в N-мерном пространстве больше порогового значения;

● мера близости между полученным N-мерным вектором и наиболее удаленными от центра кластеров N-мерными векторами кластеров статистической модели в N-мерном пространстве больше порогового значения.

2. Способ по п. 1, в котором получаемая веб-страница при построении статистической модели веб-страницы заведомо не содержит аномальных элементов.

3. Способ по п. 1, в котором элементами веб-страницы, о содержимом которых собирают сведения, являются элементы, по меньшей мере, следующих видов:

а) объекты:

- апплеты;

- скрипты;

- машинный код;

б) формы.

4. Способ по п. 3, в котором собираются сведения о содержимом по меньшей мере двух элементов веб-страницы.

5. Способ по п. 4, в котором элементы относятся к разным видам элементов.

6. Способ по п. 4, в котором элементы относятся к одному виду элементов.

7. Способ по п. 1, в котором для создания кластера используют иерархические методы.

8. Способ по п. 7, в котором кластер создают агломеративным методом, в котором наиболее близкие по расстоянию N-мерные векторы элементов выделяются в кластеры или наиболее близкие по расстоянию кластеры объединяют в один кластер.

9. Способ по п. 8, по которому расстояние: линейное, или евклидово, или обобщенное степенное Минковского, или Чебышева, или Манхэттенское.

10. Способ по п. 8, в котором наиболее близкими признаются векторы, имеющие наименьшее взаимное расстояние.

11. Способ по п. 8, в котором выделяют кластер до тех пор, пока радиус кластера максимально не приблизится к пороговому значению радиуса, где максимальным приближенным является радиус, который при следующем акте выделения кластера превысит пороговое значение радиуса.

12. Способ по п. 8, в котором выделяют кластер до тех пор, пока не останется кластеров или векторов с допустимой мерой близости, где допустимой мерой близости считается мера, не превышающая установленное пороговое значение.

13. Способ по п. 8, в котором наиболее близкими признаются кластеры, имеющие

RU 2016136226 A

RU 2016136226 A

наименьшее расстояние между центрами.

14. Способ по п. 7, в котором кластер создают дивизимным методом, где кластер образуют векторы, взаимное расстояние которых меньше предельно допустимого расстояния, при этом предельная допустимость расстояния определяется пороговым значением.

15. Способ по п. 14, в котором отделяют кластеры до тех пор, пока радиус кластера не станет равным или меньше порогового значения радиуса.

16. Способ по п. 1, в котором для создания кластера используют неиерархические методы.

17. Способ по п. 1, в котором аномальным является элемент или группа элементов, N-мерный вектор которых не соответствует построенной статистической модели веб-страницы, а именно не принадлежит ни одному из кластеров модели.

RU 2016136226 A

RU 2016136226 A