РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2017 105 763** (13) **A**

(51) МПК
G06F 21/50 (2013.01)
G06F 21/56 (2013.01)
G06F 21/60 (2013.01)

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2017105763, 25.08.2015**

Приоритет(ы):
(30) Конвенционный приоритет:
24.09.2014 US 14/495,692

(43) Дата публикации заявки: **21.08.2018** Бюл. № **24**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **21.02.2017**

(86) Заявка PCT:
US 2015/046826 (25.08.2015)

(87) Публикация заявки PCT:
WO 2016/048544 (31.03.2016)

Адрес для переписки:
109012, Москва, ул. Ильинка, 5/2, ООО "Союзпатент"

(71) Заявитель(и):
МАКАФИ, ИНК. (US)

(72) Автор(ы):
ДЖОХРИ Амританшу (IN),
СИНГХ Балбир (IN),
КХУРАНА Джаскаран (IN),
ПАНДЕЙ Ратнеш (IN)

(54) НЕРАЗРУШАЕМЫЙ БЕЛЫЙ СПИСОК

(57) Формула изобретения

1. Вычислительное устройство, содержащее:
накопитель, содержащий исполняемый объект; и
один или более логических элементов, содержащих механизм безопасности для:
обнаружения, что исполнительный объект попытался выполнить действие;
перехвата указанного действия;
назначения репутации указанному действию; и
осуществления действия, в соответствии с указанной репутацией.

2. Вычислительное устройство по п. 1, в котором осуществление действия, в соответствии с репутацией, содержит подэтап, на котором: разрешают исполнительному объекту выполнить действие.

3. Вычислительное устройство по п. 1, в котором осуществление действия, в соответствии с репутацией содержит подэтап, на котором блокируют исполняемый объект, не разрешая выполнять ему действия.

4. Вычислительное устройство по п. 1, в котором осуществление действия, в соответствии с репутацией, содержит подэтап, на котором: предоставляют предупреждение пользователю.

5. Вычислительное устройство по п. 1, в котором осуществление действия в соответствии с репутацией содержит подэтап, на котором принимают решение пользователя, относящееся к действию.

RU 2017105763 A

RU 2017105763 A

6. Вычислительное устройство по п. 5, в котором механизм репутации дополнительно выполнен с возможностью размещения в кэш решения пользователя.

7. Вычислительное устройство по п. 1, в котором назначение репутации для выполнения действия содержит использование эвристических подходов.

8. Вычислительное устройство по п. 1, в котором назначение репутации для действия содержит подэтапы, на которых:

идентифицируют тип объекта;

рассчитывают проверочную сумму для объекта; и

выделяют атрибуты объекта.

9. Вычислительное устройство по п. 1, в котором назначение репутации для действия содержит подэтап, на котором: консультируются в базе аналитических данных об угрозе.

10. Вычислительное устройство по п. 1, в котором назначение репутации для действия содержит подэтап, на котором: обнаруживают пакет запроса ввода/вывода.

11. Вычислительное устройство по п. 1, в котором назначение репутации содержит подэтап, на котором: предоставляют самоудостоверение.

12. Вычислительное устройство по п. 1, в котором выполнение действия в соответствии с репутацией содержит подэтап, на котором: обнаруживают и исключают ложноположительные суждения.

13. Вычислительное устройство по п. 12, в котором обнаружение и исключение ложноположительных суждений содержит подэтапы, на которых: определяют, что для исполнительного объекта была получена предварительная выборка, и разрешают получение предварительной выборки без запроса решения пользователя.

14. Один или более считываемые компьютером носителей, хранящий выполнимые инструкции, вызывающие выполнение процессором функционирования для:

обнаружения, что выполнимый объект попытался выполнить действие;

перехвата действия;

назначения репутации действию; и

выполнения действия, в соответствии с указанной репутацией.

15. Один или более считываемых компьютером носителей информации по п. 14, в котором действие, в соответствии с репутацией, содержит подэтап, на котором: разрешают исполнительному объекту выполнить действие.

16. Один или более считываемых компьютером носителей информации по п. 14, в котором действие, в соответствии с репутацией содержит подэтап, на котором блокируют исполнительный объект, не разрешая выполнять ему действия.

17. Один или более считываемых компьютером носителей информации по п. 14, в котором действие, в соответствии с репутацией, содержит подэтап, на котором: предоставляют предупреждение пользователю.

18. Один или более считываемых компьютером носителей информации по п. 14, в котором действие, в соответствии с репутацией, содержит подэтап, на котором: принимают решение от пользователя, относящееся к действию.

19. Один или более считываемых компьютером носителей информации по п. 18, в котором инструкции дополнительно вызывают выполнение процессором размещения в кэше решения пользователя.

20. Один или более считываемых компьютером носителей информации по п. 14, в котором назначение репутации для действия содержит подэтапы, на которых:

идентифицируют тип объекта;

рассчитывают проверочную сумму для объекта; и

выделяют атрибуты объекта.

21. Один или более считываемых компьютером носителей информации по п. 14, в

RU 2017105763 A

RU 2017105763 A

котором назначение репутации для действия содержит подэтап, на котором: обнаруживают пакет запроса ввода/вывода.

22. Один или более считываемых компьютером носителей информации по п. 14, в котором выполнение действия в соответствии с репутацией содержит подэтап, на котором: обнаруживают и исключают ложноположительные суждения.

23. Один или более считываемых компьютером носителей информации по п. 22, в котором обнаружение и исключение ложноположительных суждений содержит подэтапы, на которых: определяют, что для исполнительного объекта была получена предварительная выборка, и разрешают получение предварительной выборки без запроса решения пользователя.

24. Способ, содержащий этапы, на которых:

обнаруживают, что исполнительный объект попытался выполнить действие;

перехватывают указанное действие;

назначают репутацию для указанного действия; и

выполняют действие, в соответствии с указанной репутацией.

25. Способ по п. 24, в котором выполнение действия в соответствии с репутацией содержит подэтап, на котором: обнаруживают и исключают ложноположительные суждения.

RU 2017105763 A

RU 2017105763 A