

(12) МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В
СООТВЕТСТВИИ С ДОГОВОРом О ПАТЕНТНОЙ КООПЕРАЦИИ (РСТ)

(19) Всемирная Организация
Интеллектуальной Собственности
Международное бюро

(43) Дата международной публикации
30 декабря 2021 (30.12.2021)



(10) Номер международной публикации
WO 2021/262025 A1

(51) Международная патентная классификация:
G06F 21/56 (2013.01)

(21) Номер международной заявки: РСТ/RU2020/000319

(22) Дата международной подачи:
30 июня 2020 (30.06.2020)

(25) Язык подачи: Русский

(26) Язык публикации: Русский

(30) Данные о приоритете:
2020121186 26 июня 2020 (26.06.2020) RU

(71) Заявитель: **ОБЩЕСТВО С ОГРАНИЧЕННОЙ
ОТВЕТСТВЕННОСТЬЮ "ГРУППА АЙБИ ТДС"**
("GROUP IB TDS" LTD.) [RU/RU]; Территория Ин-

новационного Центра Сколково, Большой бульвар, 42,
стр. 1, эт. 0, пом. 263 Москва, 121205, Moscow (RU).

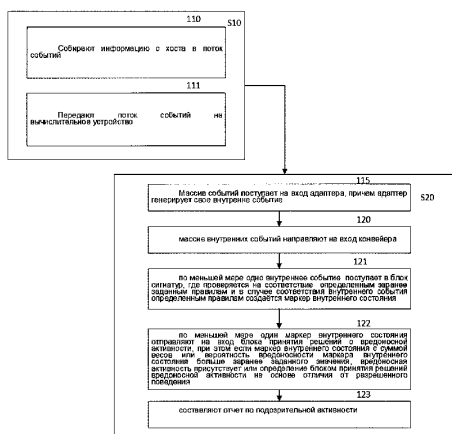
(72) Изобретатели: **ПЕРФИЛЬЕВ, Сергей Сергеевич**
(**PERFILYEV, Sergey Sergeevich**); ул. Чайникова, д.
29 Пермский край, гор. Лысьва, 618900, Permskiy kraj,
gor. Lys'va (RU). **АНДРЕЕВ, Николай Николаевич**
(**ANDREEV, Nikolay Nikolaevich**); ул. Молодежная,
д. 70, кв. 205 Московская обл., г. Химки, 141410,
Moskovskaya obl., g. Khimki (RU).

(74) Агент: **КОТЛОВ, Дмитрий Владимирович**
(**KOTLOV, Dmitry Vladimirovich**); ООО "ЦИС "Скол-
ково", Территория инновационного центра "Сколково",
4, оф. 402.1 Москва, 143026, Moscow (RU).

(81) Указанные государства (если не указано иначе, для
каждого вида национальной охраны): AE, AG, AL, AM,

(54) Title: DETECTING MALICIOUS ACTIVITY BY ANALYSING THE BEHAVIOUR OF OBJECTS IN A NON-ISOLATED ENVIRONMENT

(54) Название изобретения: ОПРЕДЕЛЕНИЕ ВРЕДНОСНОЙ АКТИВНОСТИ ПО АНАЛИЗУ ПОВЕДЕНИЯ ОБЪЕКТОВ
В НЕИЗОЛИРОВАННОЙ СРЕДЕ



Фиг. 2

110 Information from host is collected into a flow of events.

111 Flow of events is transmitted to a computer.

115 Set of events arrives at an adapter input, adapter generates its own internal event.

120 Set of internal events is sent to a signature unit, where it is checked for conformity with predetermined rules; if the internal event conforms to the rules, an internal status marker is generated.

121 At least one internal status marker is sent to an input of a decision making unit for determining malicious activity.

122 At least one internal status marker is sent to an input of a decision making unit for determining malicious activity.

123 Report is compiled concerning suspicious activity.

(57) Abstract: Claimed are a method and system for detecting malicious activity by analysing the behaviour of objects in a non-isolated environment. The method includes the steps of: collecting information into a flow of events using a detection unit; transmitting said flow of events to a computer, where the flow of events generated is analysed with respect to a predetermined amount of time, wherein an event from the flow of events is sent to the input of a finite state machine and an adapter according to the type of event, and the adapter generates its own internal event; feeding said internal event, as it is generated, into a signature unit, where the generated internal event is checked using predetermined rules, and an internal status marker is generated if the internal event conforms to said predetermined rules; sending the internal status marker to the input of a decision making unit for determining malicious activity, wherein if the internal status marker exceeds a predetermined value in terms of a sum of weights or in terms of the probability of the internal status marker being malicious, then malicious activity is present, or the decision making unit determines the presence of malicious activity on the basis of a deviation from permissible behaviour; compiling a report concerning suspicious activity.

(57) Реферат: Заявлены способ и система определения вредоносной активности по анализу поведения объектов неизолированной среде. Способ включает этапы, на которых: посредством блока обнаружения собирают информацию в поток событий; передают на вычислительное устройство поток событий, где осуществляют анализ полученного потока событий за заранее определенное количество времени, при этом событие из потока событий отправляют на вход конечному автомату адаптеру в зависимости от типа события, причем адаптер генерирует свое внутреннее событие; по мере получения события внутреннее событие подают в блок сигнатур, где осуществляют проверку полученного внутреннего события заранее заданным правилам, и в случае

[продолжение на следующей странице]

WO 2021/262025 A1

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Указанные государства (если не указано иначе, для каждого вида региональной охраны): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), евразийский (AM, AZ, BY, KG, KZ, RU, TJ, TM), европейский патент (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Опубликована:

— с отчётом о международном поиске (статья 21.3)

соответствия внутреннего события заранее заданным правилам создают маркер внутреннего состояния; маркер внутреннего состояния отправляют на вход блока принятия решений о вредоносной активности, при этом если маркер внутреннего состояния с суммой весов или вероятность вредоносности маркера внутреннего состояния больше заранее заданного значения, вредоносная активность присутствует или определение блоком принятия решений вредоносной активности на основе отличия от разрешенного поведения; составляют отчет по подозрительной активности.