РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2020616348

Программа для извлечения полезной информации из журналов событий с использованием распараллеливания вычислений

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования «Тихоокеанский государственный университет» (RU)***

Авторы: ***Москвичев Антон Дмитриевич (RU),***
Долгачев Михаил Владимирович (RU)

Заявка № **2020615399**
Дата поступления **28 мая 2020 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***16 июня 2020 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РЕФЕРАТ

Программа: Программа для извлечения полезной информации из журналов событий с использованием распараллеливания вычислений

Аннотация: Программа является модулем SIEM-системы, предназначенным для извлечения полезной информации из журналов событий от различных источников. SIEM-система – платформы для выявления угроз информационной безопасности на основе анализа журналов событий.

Программа, получив запись о событии из журнала, классифицирует ее по правилам, заранее записанным в базу данных. Далее событие перенаправляется в поток согласно своему классу и обрабатывается. Полученные результаты передаются шине данных для передачи другим модулям SIEM-системы для дальнейшего анализа.

Программа выполняет следующие функции: принимает на вход запись из журнала с неструктурированными событиями; классифицирует событие согласно правилам из базы данных; извлекает полезную информацию и передает на шину данных. Для работы программы требуются система управления базами данных MongoDB и шина данных RabbitMQ.

Язык (программирования): Golang

Объём программы: 9,94 КБ