Отзыв

на автореферат диссертационной работы Пестова Игоря Евгеньевича на тему «Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора метрик» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Современные средства защиты информации, предназначенные для обеспечения безопасности данных при их обработке в информационных системах, в настоящее время отличаются большим разнообразием. Однако в них не в полной мере проработаны решения, направленные на обеспечение безопасности данных при их обработке в облачных инфраструктурах. Диссертационная работа Пестова И.Е. имеет своей целью исследование и разработку таких решений в сфере информационной безопасности, и направленна на повышение защищенности виртуальных машин и контейнеров облачной инфраструктуры.

Нарушение конфиденциальности, целостности или доступности инстансов облачной инфраструктуры вызывает значительные убытки организации провайдера облачных услуг. Таким образом, разработка метода сбора метрик инстансов облачной инфраструктуры, для оценки состояния информационной безопасности, методики выявления аномалий на основе внутреннего аудита и мониторинга состояния метрик инстансов и облачной инфраструктуры, методика типизированной рефлексии на вредоносные управляющие воздействия, безусловно, является актуальной задачей.

В рамках диссертационной работы, первым научным результатом является: метод сбора метрик инстансов облачной инфраструктуры, для оценки состояния информационной безопасности. Предложенный метод, отличается от существующих использованием безагентного способа сбора метрик и преобразование данных метрик в формат временных рядов на этапе сбора устройствам.

Второй научный результат отражает разработанный метод выявления аномалий на основе внутреннего аудита и мониторинга состояния метрик инстансов и облачной инфраструктуры. Существенным отличием данного метода от существующих, является наличие в нем автоматизированного учета экзогенных параметров.

Как итог работы, третьим научным результатом является методика типизированной рефлексии на вредоносные управляющие воздействия. Предложенная методика отличается от известных методик, комплексной оценкой состояния инстанса. Разработанная математическая модель позволяет в полной мере учитывать поведения инстанса на основе нормального распределения и тем самым осуществлять сравнение при анализе метрик использования ресурсов с моделью прогнозирования условных периодов.

Как любая научно-квалификационная работа не лишена отдельных недостатков:

1. В автореферате недостаточно полно рассмотрены релевантные работы зарубежных ученых;

2. В автореферате не в полной мере отражено описание методики проведения экспериментов по выявлению несанкционированных управляющих воздействий.

Выявленные замечания не снижают актуальность научно обоснованных технических решений и не влияют на положительную оценку диссертационного исследования. На основе автореферата, можно сделать вывод о том, что диссертация Пестова И.Е. является законченной научной работой, в которой представлены решения актуальных задач обеспечения безопасности виртуальных машин и контейнеров. Результаты диссертационного исследования внедрены в ПАО «РОСТЕЛЕКОМ» в деятельности подразделений информационной безопасности, в ГАУ КО КГ НИЦ в мероприятиях по выработке перспективных подходов к защите информации, а также использованы в учебном процессе СПбГУТ. Разработанные решения

обладают научной новизной и позволяют обеспечить безопасность инстансов облачной инфраструктуры.

Автореферат позволяет сделать вывод о том, что диссертация Пестова И. Е. на тему «Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора метрик» соответствует требованиям ВАК России, предъявляемым к кандидатским диссертациям (п. 9 Положения о присуждении учёных степеней, утверждённого Постановлением правительства РФ от 24.09.2013 № 842, а её автор заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

К.т.н., доцент, доцент кафедры
информационных технологий
и организации расследования киберпреступлений
ФГКОУ ВО «Санкт-Петербургская академия
Следственного комитета Российской Федерации»

[redacted] КИСЕЛЕВ Олег Николаевич

«12» декабря 2022 г.

[redacted]

Подпись заверяю
Инспектор отделения кадров
[redacted] Тетёрина Ю.В.
Федеральное государственное казенное образовательное учреждение высшего образования «Санкт-Петербургская академия Следственного комитета Российской Федерации»
«12» 12 2022 г.

Федерального государственного казенного образовательного учреждения высшего образования «Санкт-Петербургская академия Следственного комитета Российской Федерации».
190000, г. Санкт-Петербург, набережная реки Мойки, д. 96,
e-mail: *kiselev.o.n@skspba.ru*