Отзыв на автореферат
диссертации Смирнова Дмитрия Владимировича
«Методы поиска признаков инсайдера в Big Data»,
представленной на соискание ученой степени
кандидата технических наук по специальности
05.13.19 – Методы и системы защиты информации,
информационная безопасность

Задача обнаружения инсайдера является одной из самых сложных и важных в круге проблем, связанных с обеспечением информационной безопасности. Недостаточное внимание корпораций к этой области не раз приводило к значительным финансовым и репутационным потерям. Деятельность инсайдеров и противодействующих им отделов защиты информации подобна гонке вооружений: каждая из сторон разрабатывает новые подходы и алгоритмы. В связи с ростом объема хранимых данных предъявляются новые требования к эффективности алгоритмов выявления инсайдерства. По этим причинам данное исследование крайне актуально.

В диссертационной работе Д. В. Смирнова предложены алгоритмы поиска признаков инсайдерской активности в хранимой информации о взаимодействии пользователей с большим хранилищем данных. Показана работоспособность этих алгоритмов в ситуации, когда эта информация постоянно пополняется новыми сведениями, а время анализа жестко ограничено.

Разработан алгоритм интеллектуального анализа данных, обеспечивающий эффективный первичный поиск в неразмеченных данных сведений, релевантных идентификации признаков вредоносных инсайдерских активностей. Он включает в себя профиль угроз, содержащий типичные сценарии инсайдерских атак. Профиль угроз динамически пополняется новыми данными об угрозах и дополняется диаграммой сходств типовых сценариев угроз.

Алгоритм первичного поиска дополняется статистическими алгоритмами идентификации и анализа аномалий поведения объектов мониторинга, а также алгоритмами оценки качества и надежности формируемых статистическими средствами заключений о классификации аномалий в поведении объектов мониторинга. Алгоритмы оценивания угроз служат формированию дополнительных оснований для принятия решений о приоритетности отработки выявленных ситуаций, содержащих возможные угрозы инсайдерских действий.

Сговор инсайдеров выявляется специальным алгоритмом, использующим статистический анализ в сочетании с кластеризацией.

Важным результатом работы является разработка программного комплекса, включающего в себя набор сервисных программных инструментов, поддерживающих нормализацию данных как в первичном, так и во вторичном поиске; набор оригинальных программных инструментов формирования и реконструкции диаграммы сходств типовых сценариев используемого профиля угроз; проблемно-ориентированные средства имитационного моделирования для оценки ряда эффектов и поддержки принятия управленческих решений; разработки по интеграции этих новых программных инструментов с уже имеющимися в организации промышленными программными инструментами обработки данных.

Достоверность результатов исследования, работоспособность и результативность предложенных алгоритмов подтверждается промышленной реализацией программных инструментов в деятельности крупной коммерческой организации, а также согласованностью с данными, имеющимися в отечественной и зарубежной литературе.

Основные результаты работы докладывались и обсуждались на различных научных семинарах и конференциях.

Д. В. Смирнов опубликовал 7 научных работ по теме диссертации, в том числе 6 в изданиях из перечня ВАК, 4 в изданиях, индексированных в базах SCOPUS. Получены 2 свидетельства о регистрации программ для ЭВМ и баз данных.

Судя по автореферату, диссертация «Методы поиска признаков инсайдера в Big Data» полностью соответствует требованиям Положения о порядке присуждения ученых степеней ВАК Минобрнауки РФ, а ее автор – Д. В. Смирнов – заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Профессор кафедры
высшей математики
Новосибирского государственного
технического университета
доктор физико-математических
наук, доцент Ковалевский Артем Павлович

«01» 12 2021 года

Подпись профессора кафедры высшей математики НГТУ
д.ф.-м.н., доцента А. П. Ковалевского заверяю

Начальник отдела кадров НГТУ О. К. Пустовалова

Ковалевский Артем Павлович, доктор физико-математических наук по специальности 05.13.17 – теоретические основы информатики, доцент, профессор кафедры высшей математики Федерального государственного бюджетного образовательного учреждения высшего образования «Новосибирский государственный технический университет» (НГТУ),
630073, г. Новосибирск, пр. Карла Маркса, 20,
телефон: (383) 346-08-43
факс: (383) 346-02-09
адрес электронной почты: rector@nstu.ru
веб-сайт: http://www.nstu.ru

Контактные данные:
телефон: (383) 346-32-26
адрес электронной почты: kovalevskij@corp.nstu.ru