ОТЗЫВ

научного руководителя на диссертационную работу

Смирнова Дмитрия Владимировича «Методы поиска признаков инсайдеров в BigData», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (технические науки)

Смирнов Дмитрий Владимирович окончил Московский Государственный Институт Электронной Техники (ТУ) в 2008 году по специальности «Комплексная защита объектов информатизации». С 2009 года работал ведущим аналитиком в области информационных систем и инфраструктуры в ЗАО «Банк Кредит Свисс». С 2012 года является сотрудником службы безопасности Сбербанка. В ноябре 2020 года был прикреплен к ФИЦ ИУ РАН для подготовки кандидатской диссертации.

Смирнову Д. В.научным руководителем была поставлена очень актуальная, но сложная научно-техническая задача по разработке методов поиска признаков враждебной деятельности инсайдеров в больших данных мониторинга работы множества пользователей с информацией в общем хранилище информационных ресурсов организации.

Поиск в больших данных мониторинга порождает большое количество «ложных тревог», но любые методы сокращения ложных тревог приводят к потере истинных признаков инсайдеров. Отсюда у Смирнова Д.В. возникла идея двухуровневой архитектуры системы поиска, предполагающей на первом этапе увеличение числа ложных тревог, но не теряющей истинных признаков. Для борьбы с ложными тревогами Смирнов Д.В.использовал информацию из нескольких информационных пространств. Этот подход позволил сопоставлять результаты обработки информации в различных информационных пространствахдруг с другом. Этот метод и ряд кластерных подходов совместно со статистическими и интеллектуальными методами анализа промежуточных результатов позволили получать хорошие результаты. Все методы фильтрации данных рассматривались на предмет эффективности выявления вкраплений признаков инсайдерской активности. Для оценок

эффективности использовались вероятностные методы. Если вероятность случайного появления выявленной эмпирической закономерности достаточно значима, то необходимо искать дополнительную информацию для подтверждения найденной закономерности. Один из таких результатов – условия выявления сговора инсайдеров.

Важный результат диссертации состоит в организации выявления признаков инсайдеров в различных информационных пространствах. Смирновым Д. В. предложено, а затем технически реализовано проведение поиска с помощью текущего перечня угроз, состоящего из множества типовых сценариев. Для преодоления барьера сложности реализации алгоритма пришлось привлечь достаточно серьезные результаты из теории частично-упорядоченных множеств. Экспериментальная проверка на реальных данных показала практическую работоспособность методов в реальных условиях.

При работе над решением проблем промышленной реализации поиска признаков деятельности инсайдера оригинальное решение получила задача нормализации данных, что позволило значительно сократить трудоемкость результирующего алгоритма. Следующие этапы поиска состояли в обеспечении приемлемых условий для работы оперативных сотрудников с разумно ограниченной по объему базой данных.

Создание программного обеспечения проводилось в два этапа. Сначала Смирнов Д.В. сам создавал программы для проверки правильности и работоспособности алгоритмов, а на втором этапе участвовал в создании промышленного программного комплекса. При создании промышленного комплекса Смирнов Д.В. решал вопросы архитектуры комплекса средств поиска признаков инсайдерской деятельности, принимал участие в создании программ, алгоритмов и требований к параметрам программ, а также вносил изменения для обеспечения выполнения требований по времени и создания удобных интерфейсов. Промышленный комплекс показал хорошие технические результаты и позволил решить успешно ряд оперативных задач по поиску

инсайдеров. По этим результатам Смирнов Д. В. получил акт о внедрении результатов диссертации.

По мнению научного руководителя Смирнов Д.В. провел большую исследовательскую работу, которая показала его высокую квалификацию и умение решать сложные научно-технические и научно-организационные задачи с привлечением различных областей знаний. Для достижения теоретических и практических результатов Смирнов Д. В. изучил большой объем научной литературы и умело воспользовался консультациями с ведущими учеными, в том числе в ФИЦ ИУ РАН.

Считаю, что диссертация Смирнова Д.В. удовлетворяет всем квалификационным требованиям ВАК, предъявляемым к кандидатским диссертациям, а сам соискатель заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Научный руководитель
главный научный сотрудник
Федерального исследовательского центра
«Информатика и управление» РАН,
доктор физико-математических наук,
профессор Грушо Александр Александрович
08.06.2021

Подпись Грушо А.А.
Заверяю Захаринный А.А.