ПАО Сбербанк
117997, Москва, ул. Вавилова, д. 19
Т +7 (495) 500 55 50, +8 (800) 555 55 50
sber@sber.ru, sber.ru

№ б/н 01 декабря 2021г.

на №

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

Диссертационная исследование Д.В.Смирнова посвящено актуальной и востребованной тематике – обеспечению защиты от различных вредоносных воздействий крупных бизнес-систем, на постоянной основе оперирующих так называемыми большими данными (Big Data). Выбрав для углубленного анализа в качестве основной проблематики задачу оперативной идентификации в постоянно пополняемых новой информацией Big Data признаков вредоносных инсайдерских активностей и организации противодействия их влиянию, автор разработал и внедрил в практику бизнес-деятельности крупного отечественного коммерческого банка проблемно-ориентированную методику поиска признаков инсайдера вместе с реализующим ее программно-техническим комплексом.

С точки зрения бизнес-приложений анализируемая в диссертационной работе проблематика имеет несколько принципиально значимых отличительных особенностей. Прежде всего, это – необходимость оперировать постоянно дополняемыми новой информацией массивами данных, в том числе – обеспечить на постоянной основе мониторинг исходных – неразмеченных (так называемых «сырых») – данных. Реальные объемы подобных данных в крупных коммерческих банках таковы, что их оперативный анализ прямым применением современных коммерческих программных систем оказывается трудно-реализуемым: подсистемы обновления поисковых индексов в ряде случаев попросту не справляются с текущим потоком вновь поступающих первичных данных.

Не менее критичным оказывается требование обеспечить анализ уже полученных новых данных в жестко ограниченное время: уже пришедший пул данных должен быть обработан до получения очередного обновления (например, данных закрываемого операционного дня и т.п.).

Наконец, все формируемые в ходе выполняемого мониторинга Big Data заключения об идентификации инсайдерских угроз должны быть надежно обоснованы: минимизация ошибок первого и второго рода (ложных срабатываний и пропусков реальных угроз) критически значима для обеспечения эффективности расхода ресурсов, которые требуются для работы подобной системы защиты бизнеса от вредоносных воздействий.

Разработанные автором диссертационного исследования методика и программно-технический комплекс идентификации инсайдерских угроз предлагают оригинальное и эффективное решение для преодоления каждого из названных выше барьеров. Используя современные достижения в области компьютерного анализа данных – методы искусственного интеллекта, комбинируемые со специальными математическими методами статистического анализа данных, Д.В.Смирнов разработал технологию, которая позволяет эффективно выявлять порождаемые инсайдерскими активностями аномалии – малые

вредоносные «вкрапления» в Big Data, идентификация которых и предъявляет признаки инсайдерской активности.

Задействованные автором диссертационной работы технологии искусственного интеллекта позволяют сделать результаты такой идентификации объясняемыми и понятными работникам служб безопасности, отвечающим за результаты выполняемого мониторинга. При этом сам процесс мониторинга и фильтрации Big Data организован так, чтобы обеспечить оперативный анализ больших - более 1200 серверов и 100 информационных ресурсов в крупном отечественном коммерческом банке - объемов разнотипной информации о действиях большого числа пользователей.

Предложенные автором диссертационного исследования технологические решения позволяют выстроить весь процесс фильтрации Big Data и мониторинга инсайдерских угроз так, чтобы не выходить за рамки определяемых основным бизнесом банка ресурсных ограничений по бюджетам, срокам и численности персонала, привлекаемого для борьбы с вредоносными инсайдерскими активностями.

По теме диссертации автором подготовлены 7 публикаций: 6 – в изданиях из перечня ВАК, 4 - в изданиях, индексированных в базах SCOPUS. Разработанные диссертантом ключевые программные продукты комплекса ИТ-решений, реализующего предложенную им методику противодействия вредоносным действиям инсайдеров, защищены двумя авторскими свидетельствами о регистрации программ для ЭВМ и баз данных.

Практическая значимость предложенных решений подтверждена актами об их внедрении в операционную деятельность крупного отечественного коммерческого банка.

К содержанию автореферата нет замечаний принципиального характера.

Судя по автореферату, рассматриваемая диссертация «Методы поиска признаков инсайдера в Big Data» полностью соответствует требованиям «Положения о присуждении ученых степенней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 № 842 (в редакциях Постановлений Правительства РФ № 335 от 21.04.2016, № 748 от 02.08.2016, № 650 от 29.05.2017, № 1024 от 28.08.2017, № 1168 от 01.10.2018, № 426 от 20.03.2021, с изменениями, внесенными Постановлением Правительства РФ № 751 от 26.05.2020), предъявляемым к диссертациям на соискание ученой степени кандидата наук, 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.

Старший управляющий директор –
директор Департамента управления данными
ПАО Сбербанк
к.т.н.

Б.И. Рабинович

«01» декабря 2021 года
Подпись Старшего управляющего директора –
директора Департамента управления данными
ПАО Сбербанк Б.И. Рабиновича удостоверяю

Подлинность подписи
ЗАВЕРЯЮ
Старший специалист
Организационно-административного
управления Департамента управления
делами ПАО Сбербанк
И.П.Рословцева
СБЕРБАНК
г. Москва