Отзыв на автореферат

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

Анализ больших объемов данных (BigData) в ограниченное время вошел сегодня в круг актуальных направлений исследований и разработок в области кибербезопасности. Одной из проблем является оперативная идентификация признаков вредоносных инсайдерских активностей и организация эффективного противодействия им. Особого внимания требует разработка алгоритмов решения таких задач в крупных коммерческих банках, где кража конфиденциальных данных (персональной информации, сведений об остатках на счетах, содержимом портфеля ценных бумаг, данных о движении средств по счету и т.п.) позволяет злоумышленникам осуществлять преступные посягательства на физических и юридических лиц, собирать информацию о конкурирующих фирмах и т.д.

Анализируемые в диссертационной работе Д.В. Смирнова инсайдерские угрозы – это вредоносные активности, которые исходят от сотрудников внутри организации (периметра защиты), в частности – от действующих работников, бывших работников, подрядчиков, деловых партнеров и даже завербованных работников или работников, специально внедренных в организацию, которые обладают доступом к конфиденциальной информации по своим должностным обязанностям и которые имеют представление о системе управления информационной безопасностью организации. Поиск признаков действий инсайдеров в BigData в условиях регулярного обновления таких данных, выполняемый при временных ограничениях на анализ данных и принятие решений, представляет актуальную и практически значимую научно-техническую задачу обеспечения информационной безопасности.

Автором реализован подход, который основан на том, что инсайдеры порождают аномалии – малые вредоносные «вкрапления» в BigData, – по которым удается выявлять признаки их активности. При этом необходимо, чтобы сформированные в процессе выполняемого компьютерного анализа реко-

мендации были объясняемы и понятны экспертам по противодействию инсайдерским активностям – работникам оперативных служб безопасности, на которых в конечном итоге ложится ответственность за принятые решения и их последствия.

В рамках предложенного решения поставленной научно-технической проблемы разработаны методы и программные «инструменты» работы с большими объемами (более 1200 серверов и более 100 информационных ресурсов на реальном объекте защиты – в крупном отечественном коммерческом банке) гетерогенной информации о действиях большого числа пользователей, позволяющие выделять без потерь в мониторимых данных описания тех взаимодействий, которые несут потенциальные или же явные риски вредоносных последствий, а также эффективным образом организовать этот процесс фильтрации BigData. Для этого были разработаны специальные процедуры сокращения объемов детально анализируемых данных, сохраняющие тем не менее в этих данных соответствующие признаки вредоносности. Процесс фильтрации организован так, чтобы оставаться в рамках соответствующих ресурсных ограничений (бюджетов, выделяемых на эти цели основным бизнесом банка; сроков выполнения каждого цикла анализа данных и принятия решений; численности персонала соответствующей квалификации в службе безопасности и др.).

Предложенная Д.В. Смирновым методика выявления вредоносных инсайдерских активностей была воплощена в специальное программно-техническое решение – комплекс ИТ-средств, ключевые элементы которого – разработанные автором данной диссертационной работы и защищенные соответствующими авторскими свидетельствами программные продукты.

По автореферату следует сделать два замечания:

1. Представленный в обзоре материала второй главы диссертационной работы подход к анализу накапливаемых в информационных пространствах сведений, который основан на математической технике полузапретов вероятностных мер, мог бы быть описан более подробно (в частности, так, как в обзоре второй главы описана используемая в анализе поведения инсайдеров статистическая техника оценки вероятности возникновения аномалий).

2. Представленное в автореферате описание ряда рассматриваемых в четвертой главе диссертации «технологических» процедур носит достаточно общий характер и, по-видимому, заслуживает дополнительных пояснений. Это упростило бы восприятие предлагаемой автором «технологической цепочки» идентификации инсайдеров.

Однако данные замечания не носят существенного характера и не могут повлиять на общую положительную оценку автореферата и диссертационной работы в целом. Судя по автореферату, рассматриваемая диссертация «Методы поиска признаков инсайдера в BigData» полностью соответствует требованиям Положения о порядке присуждения ученых степеней ВАК Министерства образования и науки 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 информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, академик РАЕН

А.С. Овчинский

«20» 12 2021 года

ПОДПИСЬ Овчинского А.С.
ЗАВЕРЯЮ
Начальник ОДиР
полковник полиции
Артамонова И.Л. _____
(подпись)
"20" 12 2021 г.