ОТЗЫВ

официального оппонента на диссертацию

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

Оценка актуальности темы. Инсайдерская активность представляет собой наиболее трудно обнаруживаемую угрозу по двум причинам 1) большая роль человеческого фактора и непредсказуемости целей; 2) трудность формирования пространства анализируемых признаков и определения критериев вредоносного влияния.

Именно поэтому, несмотря на значительное число исследований в этом направлении, отсутствует общепринятый инструментарий для обнаружения такого вида угроз и обнаружение инсайдера составляет одну из сложных задач аудита поведения пользователей и не имеет формальной постановки.

В этой связи рассматриваемая работа, направленная на обоснование и реализацию инструментария, позволяющего администратору безопасности обнаруживать инсайдерскую активность является своевременной, востребованной и актуальной. Для решения поставленной задачи фактически отказывается от формирования априорно установленных критериев инсайдеров и предлагает выявлять искомые признаки для анализа из данных о взаимодействии пользователей с хранилищем Big Data результатов аудита.

Задача сводится к разработке интеллектуальных методов анализа больших данных в заданных ограничениях по времени, позволяющих выявлять слабовыраженные аномалии поведения пользователей и фиксировать появление потенциально опасных взаимодействий.

Научная значимость диссертационного исследования, определяющая его оценку, состоит в обработке и фильтрации гетерогенной информации о действиях пользователей, формируя обнаружение аномалий в текущую интегрированную оценку.

Для решения этой задачи в работе сформулирован и решен ряд научных задач, направленный на:

1) разработку процедур сокращения объемов анализируемой информации без потерь информативности;

2) формирование реализуемого процесса отбора аномалий в ограниченное время в виде структурированной методики.

Отличительной особенностью подхода является то, что автор оперирует с Big Data как с набором пространств, обладающих различной параметризацией, что позволяет выявлять компрометирующие данные в различных базисах параметров и объединять их в единый результат.

Такой подход позволяет в определенной степени подойти к решению противоречий между количеством исходных данных с их информативностью.

Развитие этого подхода позволяет применить ряд методов, позволяющих выявлять аномалии, идентифицировать признаки инсайдеров и предложить методику формировании рекомендаций для администратора безопасности и целенаправленному противодействию атакам инсайдера.

В первой главе приведен достаточно подробный анализ работ по поиску инсайдеров. Сформулированы задачи диссертационного исследования. Основные проблемы автоматизации поиска признаков инсайдерской активности сводятся к решению двух типов задач. К первому типу относятся задачи определения условий, при которых редкие вкрапления слабо выраженных признаков деятельности инсайдеров возможно выявлять в условиях Big Data. Ко второму типу относятся задачи вычислительной сложности, связанные с поиском вкраплений в Big Data.

Во второй главе исследованы методы работы с противоречиями при выявлении аномалий в поведении пользователей, когда необходимо изменить начальную параметризацию наблюдаемых объектов, чтобы уточнять эмпирические причины появления целевых свойств. Решены задачи, позволяющие оперировать гетерогенными данными и выявлять компрометирующие инсайдера сведения в различных информационных пространствах. Для объединения выводов предложено использовать простейшие логические функции.

Третья глава содержит результаты, определяющие возможности использования статистических методов для выявления признаков инсайдеров. В задаче выявления сговора инсайдеров использованы способы сокращения объема выборки полезных данных до уровня эффективного использования статистики. В задаче выявления связей потенциально опасных событий осуществляется фильтрация эмпирических закономерностей с помощью простейших вероятностных схем.

В четвертой главе приведены результаты организации вычислений при поиске признаков деятельности инсайдеров. Автором найдена оригинальная схема поиска, основанная на перечне угроз, который состоит из большого числа простых фильтров (типовых сценариев). Новизна состоит в том, что не делается попытка снизить уровень ложных тревог, а главным считается минимизация возможности пропуска реальных признаков инсайдера. Решение достигается за счет привлечения дополнительных данных и создания новых проблемно-ориентированных фильтров. Предложенный подход позволил сократить сложность суммарной обработки данных, что позволило вложиться в требуемые нормативы. В результате автору удалось обеспечить промышленное решение задачи поиска признаков инсайдеров в большой коммерческой структуре.

Теоретические результаты направлены на обоснование достоверности и эффективности обнаружения инсайдеров в ограниченное время состоит в получении следующих оригинальных решений:

1. Оценен объем данных (данные - объекты типа малых выборок), необходимый для эффективного использования математической статистики в задаче выявления слабо выраженных вкраплений. Для этого в исходных Big Data найдены методы выделения подмножеств требуемого размера, сохраняющие свойства выборки и позволяющие не потерять возможные аномалии, связанные враждебной деятельностью инсайдеров. Найденное сокращение объема выборки позволило осуществлять выявление сговора инсайдеров и построить методы фильтрации ложных эмпирических закономерностей.

2. Впервые для идентификации признаков, связанных с враждебной деятельностью инсайдеров использованы элементы процедурной конструкции ДСМ-метода, позволившие представить знания о текущем профиле угроз в виде частично-упорядоченного множества специального вида – диаграммы сходств. С помощью такой диаграммы реализовано выявление в анализируемых Big Data простейших риск-генерирующих фрагментов. Далее движением по цепочкам частичного порядка обеспечивается прогнозирование развития угроз в текущей ситуации, что позволяет реагировать на текущую ситуацию и заранее концентрировать ресурсы на наиболее риск-опасных направлениях.

Практическая значимость работы подтверждается успешным использованием результатов диссертации в создании промышленного решения в крупной коммерческой организации и работоспособность этого программно-технического решения для поддержки деятельности оперативных работников служб безопасности по выявлению враждебной инсайдерской деятельности. Таким образом, практическая значимость состоит в решении важной научно-технической задачи обеспечения информационной безопасности в противодействии атакам инсайдеров.

Вышесказанное позволило заключить, что работа посвящена решению актуальной проблемы и выполнена на достаточно высоком теоретическом уровне и (что весьма существенно) практически реализована и используется, что подтверждено соответствующими документами.

Тем не менее по содержанию и оформлению работы возникают следующие вопросы:

1) В работе неоднократно упоминается о временных ограничениях без указания конкретных значений. Можно ли оценить общий промежуток времени для обнаружения инсайдера и сравнить его с аналогичными решениями?

2) В реферате (стр. 3) упоминается об эффективности разрабатываемых методов фильтрации инсайдеров. Могут ли быть приведены какие-либо оценки?

3) По каким причинам автор отказался от рассмотрения поведенческих методов (хотя бы при сопоставлении типовых сценариев)?

4) Вопросы генерации новых типовых сценариев и вопросы динамического переключения на новые актуальные угрозы в диссертации носят описательный характер.

5) В автореферате недостаточно четко отражены алгоритмы вероятностных методов отбраковки случайных эмпирических закономерностей.

Указанные недостатки скорее определяют направления дальнейших исследований и не влияют на общую оценку работы. Несмотря на указанные недостатки, диссертация производит хорошее впечатление. Тема диссертации соответствует паспорту специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность. Автореферат правильно отражает содержание диссертационной работы.

Диссертация представляет собой законченное научно-квалифицированное исследование, содержащее научные и практические результаты в решении актуальной задачи обнаружения и предотвращения инсайдерской деятельности и удовлетворяет требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук в части пунктов 11, 13, 14 и 18 Постановления Правительства Российской Федерации от 24.09.2013 № 842 «О порядке присуждения ученых степеней», а ее автор – Смирнов Дмитрий Владимирович заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
Профессор Института кибербезопасности и защиты информации СПбПУ,
Профессор, доктор технических наук, 05.13.19 – Методы и системы защиты информации, информационная безопасность
195251, г. Санкт-Петербург, ул. Политехническая, д. 29, ауд. 173;
Тел. +7 (812) 552-76-32, Адрес в сети Интернет: http://ibks.spbstu.ru,
Электронная почта: kafedra@ibks.spbstu.ru.

Зегжда Петр Дмитриевич

«01» 12 2021 г.

УДОСТОВЕРЯЮ
Ведущий специалист
по кадрам
«01» 12 2021 г.