УТВЕРЖДАЮ
Ректор Томского государственного университета систем управления и радиоэлектроники
доктор технических наук, доцент
Рулевский В.М.

«30» ноября 2021 г.

ОТЗЫВ

ведущей организации на диссертационную работу

Смирнова Дмитрия Владимировича «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

Диссертация Смирнова Д.В. посвящена разработке методов выявления признаков инсайдерской активности в данных мониторинга действий пользователей большой корпоративной системы. Диссертация отражает исследования по созданию и обеспечению успешного функционирования системно-технического решения для поддержки деятельности оперативных работников служб безопасности по выявлению признаков враждебной инсайдерской деятельности.

Актуальность темы диссертации

Несмотря на то, что борьба с действиями инсайдеров в информационных системах ведется несколько десятков лет, актуальность проблемы только увеличивается. В настоящее время все крупные организации работают в условиях Big Data, где проще маскировать враждебную деятельность и легче потерять истинные признаки инсайдерской активности. Поэтому

инсайдерские атаки наносят наибольший экономический вред организациям среди других путей реализаций угроз. Поиск инсайдерских действий в Big Data данных мониторинга в условиях технических и временных ограничений является важной задачей обеспечения информационной безопасности.

Содержание диссертации

В первой главе приведен анализ работ по классификации инсайдеров и применяющимся методам поиска признаков инсайдерской деятельности. Сформулированы задачи требующие разработки новых методов. Прежде всего это задачи определения условий, при которых слабо выраженные признаков деятельности инсайдеров возможно с достаточной надежностью выявлять в условиях Big Data. Далее необходимо искать пути преодоления проблем вычислительной сложности, связанные с поиском вкраплений признаков инсайдерской деятельности в Big Data.

Вторая глава содержит результаты по разработке методов изменения параметризации наблюдаемых объектов, которые необходимо использовать для баланса снижения сложности алгоритмов обработки данных и определения эмпирических закономерностей, описывающих признаки инсайдеров. Разработаны методы, позволяющие работать с гетерогенными данными и выявлять признаки инсайдера в различных информационных пространствах. Результаты анализа данных в различных пространствах можно интегрировать с помощью методов математической логики.

Третья глава содержит результаты исследований возможности выявления сговора инсайдеров. В основе решения использованы способы сокращения объема выборки данных до уровня, когда становится возможным использование математической статистики. В этой главе приведены результаты по оценкам возможностей случайного возникновения эмпирических закономерностей, указывающих на деятельность инсайдеров.

В четвертой главе приведены результаты по архитектуре организации вычислений при поиске признаков деятельности инсайдеров. Поиск основан на двухуровневой схеме. На первом уровне проводится фильтрация Big Data, основанная на перечне угроз. Этот перечень может динамически корректироваться и состоит из множества простых фильтров (типовых сценариев). Главными задачами на этом уровне являются скорость вычислений и минимизация возможности пропуска реальных признаков инсайдера. На втором уровне фильтрация ведется с привлечением

дополнительных данных из различных информационных пространств. Значительное сокращение данных для эффективной обработки информации оперативными работниками достигнуто за счет разработки и использования алгоритмов нормализации данных. Разработанные подходы позволили сократить объем и сложность суммарной обработки данных, что позволило вложиться в требуемые нормативы.

Новизна

Новизна результатов диссертации состоит в разработке оригинальной методики аналитической оценки поведенческой активности пользователей и персонала, отличающейся от существующих возможностью в режиме ограниченного времени обрабатывать большие объемы релевантных цели поиска операционных данных.

Практическая значимость

Решена важная научно-технической задача обеспечения аспекта информационной безопасности, связанного с выявлением потенциальных внутренних злоумышленников. Созданные автором методы и алгоритмы позволили обеспечить промышленное решение задачи поиска признаков инсайдеров в большой коммерческой структуре.

Достоверность

Достоверность результатов диссертационной работы подтверждается публикациями основных результатов, согласованностью полученных результатов с аналогичными исследованиями в релевантной предметной области, апробацией на семинарах специалистов и приведенными в диссертации теоретическими и экспериментальными обоснованиями. Достоверность также подтверждается успешной реализацией проекта по созданию промышленной системы поиска признаков инсайдеров в крупной коммерческой организации.

Публикации

По теме диссертации опубликовано 7 научных статей, из них 6 - в изданиях рекомендованных ВАК, 4 из них – в изданиях, индексированных в базах SCOPUS, одна статья в рецензированном журнале. Получены свидетельства на регистрацию программ для ЭВМ и базы данных № 2021614494 «Аналитическая панель доступа данных», № 2021613506 «Поисковая система доступа к данным».

Замечания.

1). Вопросы обоснования качества фильтрации первого уровня в диссертации носят описательный характер.

2). В диссертации недостаточно четко описано функциональное взаимодействие элементов построенной архитектуры системы поиска признаков инсайдерской деятельности.

3). В автореферате недостаточно четко отражены способы использования результатов второй и третьей глав в архитектуре системы поиска признаков инсайдеров.

4) Непропорционально большая обзорная первая глава диссертации – вторая глава, начинающая представление собственных результатов, начинается со страницы 62 – почти половина работы. На наш взгляд, изучение текущего состояния проблемы, конечно, важно, но основное внимание должно уделяться изложению непосредственно полученных результатов диссертационного исследования.

5) Имеются замечания к оформлению диссертационной работы: отсутствие единообразия в оформлении, используемых шрифтах (например, в содержании, котором, содержатся не только заголовки, но и сам текст работы – весь раздел основных результатов), хаотичная расстановка абзацных отступов (например, страница 9 – «Таким образом» в начале и конце страницы – в одном месте отступ есть, во втором нет, и т.д.), непонятное использование нескольких разных типов ссылок в абсолютно идентичных ситуациях в рамках одной страницы (например, страницы 19, 20 и т.д. – в рамках одного и того же обзора одни равнозначные работы приведены внизу, другие вынесены в список литературы).

6) Приводится факт (стр. 13), что работа докладывалась на различных конференциях, однако отсутствует их перечень как во вводной части (стр. 13-14), так и в списке публикаций, что не позволяет оценить широту обсуждения полученных результатов.

Несмотря на указанные недостатки, диссертация заслуживает высокую оценку. Тема диссертации соответствует паспорту специальности 05.13.19 –

Методы и системы защиты информации, информационная безопасность. Автореферат правильно отражает содержание диссертационной работы.

Диссертация представляет собой целостное, завершенное исследование, в рамках которого решена актуальная задача повышения эффективности выявления вредоносных взаимодействий персонала с ИТ-ресурсами объекта зашиты (Big Data). Это подтверждает, что Смирнов Д.В. удовлетворяет квалификационным требованиям, предъявляемым к соискателям ученой степени кандидата наук.

Диссертация работа «Методы поиска признаков инсайдера в Big Data» удовлетворяет всем требованиям Положения о присуждении учёных степеней, а ее автор Смирнов Д.В. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв рассмотрен на заседании научного семинара каф. Комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС), протокол №11 от 26 ноября 2021 г.
Присутствовало 21 человек, из них 3 доктора наук и 10 кандидатов наук.

Проголосовало «за» 21, «против» 0, «воздержались» 0.

Председатель семинара

Зав. каф. КИБЭВС, д.т.н., проф. _____ Шелупанов А.А.

Ученый секретарь семинара, _____ Костюченко Е.Ю.
к.т.н., доцент, доцент каф. КИБЭВС

Электронная почта: saa@tusur.ru; контактный телефон: +7 (3822) 90-71-55; федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники», 634045, г. Томск, пр. Ленина 40.

Подпись Шелупанова А.А.
Костюченко Е.
УДОСТОВЕРЯЮ
Ученый секретарь
Е.В. Прокопчук