Экз. № 1

ОТЗЫВ

На автореферат диссертации Ушакова Игоря Александровича «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы. В диссертационном исследовании Ушакова И.А. решена задача разработки модельно-методического аппарата обнаружения инсайдеров в компьютерной сети на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных, что имеет важное значение для развития технологий в области информационной безопасности.

В настоящее время сформировалась потребность в обеспечении безопасного функционирования объектов критической информационной инфраструктуры Российской Федерации, большинство из которых представляют собой компьютерные сети. Эффективная деятельность по противодействию компьютерным атакам в том числе со стороны внутренних злоумышленников-инсайдеров становится все более трудоемкой и сложной задачей. Вызвано это тем, что пропускная способность каналов связи компьютерных сетей постоянно растет. В то же время аналитические возможности современных систем мониторинга и предупреждения сетевых атак (преимущественно сигнатурных) не позволяют эффективно выявлять компьютерные атаки, зашумленные большим объемом данных, передаваемых по каналам связи.

Используя новые и эффективные технологии агрегации и хранения больших объемов данных, а также организации работы системы обнаружения можно добиться нужных результатов и повысить состояние защищенности объектов критической информационной инфраструктуры.

Таким образом, диссертационное исследование считаю актуальным.

Теоретическая значимость и научная новизна диссертационной работы определяется ее вкладом в дальнейшее развитие теории и методов обеспечения информационной безопасности. В частности, автор выносит на защиту следующие положения:

1. Модель представления больших данных об инсайдерских атаках в формате NoSQL, обеспечивающая хранение и анализ признаков пользователей в компьютерных сетях в различные моменты времени.
2. Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения для обнаружения инсайдерских атак.
3. Методика обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных.

4. Архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных.

Практическая значимость заключается в следующем:

1. Модель представления больших данных об инсайдерских атаках является основой для формализации знаний о пользователях, устройствах, приложениях и сервисах, функционирующих в компьютерных сетях.

2. Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения позволяют оперировать большими объемами данных и эффективно выявлять инсайдеров. Произведена настройка алгоритмов на основе методов машинного обучения по типовым сценариям инсайдеров в компьютерных сетях. Обосновано комбинированное применение алгоритмов обнаружения инсайдеров.

3. Методика обнаружения инсайдеров повышает эффективность обнаружения внутренних злоумышленников в компьютерных сетях (оперативность повышается за счет использования методов обработки больших данных, результативность – за счет совместного использования алгоритмов на основе экспертных правил и методах машинного обучения, ресурс-экономность – за счет новых высокотехнологичных программно-аппаратных решений).

4. Архитектура и программная реализация системы способствует эффективному обнаружению инсайдеров в компьютерных сетях с использованием предложенной методики, обеспечивающей комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения.

Достоверность полученных результатов подтверждается корректностью исходных предпосылок, апробацией результатов работы на конференциях всероссийского и международного уровня, а также публикацией основных научных результатов в 40 печатных работах, в том числе 9 – в рецензируемых научных изданиях, рекомендованных ВАК при Минобрнауки России для публикации основных научных результатов диссертаций на соискание ученых степеней кандидата и доктора наук, 2 – в изданиях, индексируемых в международных базах Scopus и Web of Science, наличием 3 свидетельств о регистрации программ для ЭВМ.

Вместе с тем, следует отметить следующие недостатки:

1. В автореферате в качестве типовых сценариев атак инсайдеров были выбраны семь сценариев, однако автор не поясняет о причинах выбора именно этих сценариев, а также не аргументирует выбор именно такого количества сценариев.

2. Не до конца понятна роль обработки больших данных во втором научном результате – «Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак».

3. На рисунке 2 не указаны буквенные обозначения изображенных сущностей (I_0, I_{RB}, I_{ML}).

В целом, судя по автореферату и публикациям, диссертация Ушакова И.А., выполненная на тему: «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки

больших данных» представляет собой самостоятельную завершенную научно-квалификационную работу, в которой представлена и решена актуальная научная задача по разработке модельно-методического аппарата для обнаружения инсайдеров в компьютерных сетях на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных.

Указанные недостатки не снижают теоретической и практической ценности полученных результатов. Исследование Ушакова И.А. удовлетворяет требованиям п. 9-14 Положения о присуждении учёных степеней, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 года, предъявляемым к кандидатским диссертациям.

Считаю, что Ушаков И.А. заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Сотрудник УФСБ России по городу Санкт- Петербургу
и Ленинградскс
к.т.н., доцент ымаков Алексей Васильевич
E-mail:

Подпис
Замести у Санкт- Петербургу
и Лени

. Лебедев

"13"

№ 8/1144