ОТЗЫВ

научного руководителя о диссертационной работе
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.

Ушаков И.А., 1988 года рождения, в 2010 году с отличием окончил Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ) по специальности «Защищенные системы связи». В настоящее время работает в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН) в должности младшего научного сотрудника. В 2013 году с отличием окончил очную аспирантуру СПбГУТ.

Диссертационная работа Ушакова И.А. посвящена разработке модельно-методического аппарата для обнаружения нарушителей информационной безопасности в компьютерных сетях внутреннего периметра (инсайдеров) на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных. Основные результаты, полученные диссертантом, следующие:

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 в интересах 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.

Полученные результаты были представлены на нескольких российских и международных конференциях: международной конференции по интеллектуальным

распределенным вычислениям IDC-2019 (Санкт-Петербург, 2019), международной конференции IEEE SMARTWORLD ATC-2017 (Сан-Франциско, 2017); Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» (Санкт-Петербург, 2015, 2017, 2019), международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» в СПбГУТ (Санкт-Петербург, 2015–2019); и др.

В процессе написания кандидатской диссертации Ушаков И.А. принимал активное участие в научно-исследовательском проекте федеральной целевой программы 2019-2020 гг. «Разработка методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них».

Во время выполнения научно-исследовательской деятельности Ушаков И.А. зарекомендовал себя как грамотный научный сотрудник, способный корректно ставить и решать научные задачи, проявил самостоятельность, целеустремленность и трудолюбие при подготовке научных статей и проведении экспериментальных исследований. Выбранная диссертантом тема исследований является актуальной, а полученные им результаты соответствуют современному состоянию решаемой проблемы. Об этом свидетельствует наличие опубликованных с его авторством 9 работ, рекомендованных ВАК, и 2 работ, индексируемых в системах Web of Science и Scopus.

Ушаков И.А. является специалистом в области сетевой безопасности, технологий обработки больших данных, сертифицированным специалистом Cisco, Microsoft, VMware, что позволило ему успешно выполнить все поставленные в диссертационной работе задачи. Отмечаю его творческий подход к постановке и решению задач, инициативность и ответственность, которые характеризуют его как состоявшегося ученого в области информационной безопасности.

Полученные диссертантом теоретические результаты являются важными при решении таких задач, как разработка систем обнаружения инсайдеров.

Кандидатская диссертация Ушакова И.А. является завершенной научно-квалификационной работой, выполненной на высоком теоретическом уровне и содержащей научно обоснованные результаты в области обнаружения инсайдеров в компьютерных сетях. Данные результаты имеют весомое практическое значение, что подтверждают 3 свидетельства о регистрации программ для ЭВМ и 4 акта о внедрении

результатов диссертации в учебный процесс университетов и рабочий процесс организаций. Считаю, что диссертационная работа Ушакова Игоря Александровича полностью отвечает всем требованиям п. 9 «Положения ВАК Минобрнауки РФ», предъявляемым ВАК Министерства науки и образования России к кандидатским диссертациям, и может быть представлена к защите на диссертационном совете Д.002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Научный руководитель
Доктор технических наук, профессор,
главный научный сотрудник лаборатории проблем компьютерной безопасности
Федерального государственного бюджетного учреждения науки Санкт-Петербургского
института информатики и автоматизации Российской академии наук (СПИИРАН)

Котенко Игорь Витальевич

09 января 2020 года
Рабочий адрес: 199178, Санкт-Петербург, ВО 14 линия, дом 39
Тел. +7-(812)-328-71-81
E-mail: ivkote@comsec.spb.ru

Подпись руки _____ заверяю
Начальник отдела кадр
«09» 01 2020 г. В.Токарев