**УТВЕРЖДАЮ**
Генеральный директор
Акционерного общества «Центральный ордена
Трудового Красного Знамени научно-
исследовательский и проектно-конструкторский
институт морского флота»
к.э.н _____ С.И. Буянов
«06» 12 2019 г.

# ОТЗЫВ

**на автореферат диссертации на соискание ученой степени кандидата технических наук Коржук Виктории Михайловны на тему: «Модель и метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа» по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»**

Возросшая популярность и повсеместное применение беспроводных сенсорных сетей (БСС) способствуют не только прогрессу в области обеспечения информационной безопасности сенсорных сетей, но и увеличению к ним интереса со стороны злоумышленников. Беспроводная среда передачи данных позволяет использовать различные программно-аппаратные средства для перехвата и анализа информации, циркулирующей в сети. На существующие способы и методы защиты информации устанавливаются ограничения, связанные с особенностями сенсорных узлов: активный мониторинг, сложные алгоритмы шифрования приводят к энергетическому истощению ресурсов и, следовательно, доступность и целостность информации может быть нарушена. В соответствии с вышесказанным, работа Коржук В.М. обладает актуальностью, так как направлена на обнаружение атак сетевого уровня и учитывает поставленные ограничения.

Формализованная постановка научной задачи свидетельствует о научной грамотности соискателя и позволяет лучше понять содержание работы. В диссертации поставлена и успешно решена задача повышения эффективности идентификации атак сетевого уровня на беспроводные сенсорные сети. Положительные результаты получены благодаря использованию новой комбинации поведенческих признаков, формирующих модель профиля поведения сети, применению нового метода идентификации атак на основе комбинации алгоритмов машинного обучения и введения параметра степени

уверенности и методики идентификации, соединяющей в себе теоретические положения и практические результаты в виде элементов комплекса программного обеспечения по обнаружению вторжений.

Работа Коржук В.М. является практически значимой, поскольку представляется возможным использование не только теоретических результатов в качестве базы для дальнейших исследований, но и применение практических результатов в комплексе систем обнаружения вторжения и систем мониторинга состояния сети, а также для проектирования и внедрения в защищенные сети и системы передачи данных на основе беспроводных сенсорных сетей. Более того, результаты работы могут быть интересны не только в задачах обеспечения информационной безопасности, но и в более общих задачах классификации объектов.

Достоверность полученных результатов обеспечивается корректным использованием математического аппарата, положений математической статистики, теории информации и теории вероятности.

Как следует из реферата, диссертантом успешно решены все поставленные в диссертационном исследовании задачи. Разработанные новые методы и модели могут применяться для решения различных задач идентификации атак сетевого уровня на БСС. Результаты диссертационного исследования прошли достаточную апробацию и обсуждение на научных и научно-практических конференциях.

Необходимо отметить недостатки по автореферату:

1) Из автореферата неясно, на основании чего начинается процесс обнаружения атак: в предложенной методике (рис. 3) присутствует блок «запуск процедуры идентификации», однако не описано, достижение каких пороговых значений признаков необходимы.

2) Качество иллюстративного материала, а именно размер графиков (например, рис. 2 и рис.4), не способствует облегчению восприятия материала.

Отмеченные недостатки по содержанию автореферата не снижают качество исследований и не влияют на ценность теоретических и практических результатов диссертации.

Результаты исследований автора, судя по автореферату, отвечают в полной мере требованиям, предъявляемым к кандидатским диссертациям по специальности 05.13.19. Автореферат диссертации составлен с соблюдением установленных требований, дает полное представление о содержании работы. Основные положения выполненных

исследований нашли отражение в 3 публикациях автора, в изданиях, рекомендованных ВАК, в 8 публикациях, индексируемых Scopus и внедрены в различных научно-исследовательских проектах. Качество разработанных программных продуктов подтверждается наличием свидетельств регистрации программ для ЭВМ государственного образца.

На основании содержания автореферата, можно полагать, что представленная работа отвечает всем требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», а ее автор Коржук Виктория Михайловна заслуживает присуждения ей ученой степени кандидата технических наук.

Полное название организации: Акционерное общество «Центральный ордена Трудового Красного Знамени научно-исследовательский и проектно-конструкторский институт морского флота»

Сокращенное название организации: АО «ЦНИИМФ»

Заведующий отделом
Информационных технологий
кандидат военных наук, доцент
Юрин Игорь Валентинович

191015, Россия, Санкт-Петербург,
ул. Кавалергардская, д.6, лит.А.
Раб. тел. 8(812) 271-12-20
E-mail: YurinIV@cniimf.ru
06 декабря 2019 года

Подлинность подписи
Юрина Игоря Валентиновича
ЗАВЕРЯЮ
Заведующий отделом труда и кадров
Т.Н. Пастущак 06.12.2019