

## ОТЗЫВ

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

В настоящее время, благодаря прогрессу в области автоматизированных систем и, в частности, кибер-физических систем, широкое распространение получают сети маломощных беспроводных сенсорных устройств. В то же время, из-за использования таких устройств в медицине, управлении производством и в других областях, в условиях передачи информации по открытым каналам связи и существования широкого ряда программно-аппаратных устройств перехвата и анализа информации, возникает необходимость обеспечения информационной безопасности таких сетей. Соответственно, этим обусловлена актуальность рассматриваемой работы.

Существует большое количество разнообразных систем мониторинга состояния сетей и систем обнаружения вторжений в сетях. Однако беспроводные сенсорные сети имеют ряд ограничений, связанных с малыми объемами памяти и энергоресурсов устройств. Предложенные в работе модель и метод идентификации атак учитывают эти ограничения и позволяют определить большее, чем в других работах, количество атак на беспроводные сенсорные сети. Решение задачи повышения эффективности идентификации атак рассматривается в условиях исследования сетевого уровня модели OSI и при различных топологиях сети.

К достоинствам диссертационной работы можно отнести формализованную постановку научной задачи, исследование различных алгоритмов анализа данных применительно к рассматриваемой задаче, большое количество экспериментов, выполненных с использованием разработанных автором программных средств и направленных на подтверждение предположений автора исследования, наглядность полученных данных.

Полученные автором результаты могут служить основой для разработки мобильных программно-аппаратных средств мониторинга состояния беспроводных сенсорных сетей.

Результаты, полученные в диссертационной работе, апробированы на российских и международных конференциях, в тексте публикаций в журналах ВАК и Scopus, а также в свидетельствах о регистрации программ для ЭВМ. Более того, результаты работы были внедрены в проектной и образовательной деятельности. Соответственно, работа обладает научной новизной и практической значимостью

К автореферату могут быть предъявлены следующие замечания:

1) В тексте автореферата приведен перечень анализируемых атак, однако отсутствует их описание и соответствующие изменения в используемых для идентификации признаков.

2) В процесс идентификации введен показатель степени уверенности, однако не приведено его математическое выражение. В блок-схеме алгоритма обнаружения вторжений (рис.1) 9 блок вместо обновления параметра степени уверенности указано обновление степени уверенности.

Указанные недостатки не влияют на общую положительную оценку работы. Работы выполнена в соответствии п.9 «Положения о присуждении ученых степеней», утвержденного постановлением Российской Федерации от 24 сентября 2013 г. № 842. Считаю, что Коржук В.М. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АО «Диаконт»,  
ведущий инженер,  
к.т.н

20.11.2019

Сыров Александр Александрович

*Сергисъ Сырова А.А. удостоверяю*

МЕНЕДЖЕР ПО ПЕРСОНАЛУ  
ЧЕРКАСОВА В.А.

Адрес: г. Санкт-Петербург, ул. Учительская, дом 2

Тел.: (812) 334-00-81 (доб.4397)

Email: syrov@diakont.com