

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»

Диссертационная работа Коржук В.М. посвящена обеспечению информационной безопасности беспроводных сенсорных сетей. Данная область характеризуется повышенным интересом не только со стороны специалистов по информационной безопасности, но и со стороны разработчиков и проектировщиков защищенных систем автоматизации управления и производства, поскольку объединяет в себе беспроводные устройства мониторинга, устройства-актуаторы и открытый канал связи.

На сегодняшний день основным недостатком систем обнаружения вторжений в беспроводные сенсорные сети является малое количество идентифицируемых атак и применение активного мониторинга состояния сети, что в контексте ресурсных ограничений беспроводных сенсорных сетей может привести к уменьшению времени корректной работы устройств, и, следовательно, к нарушениям целостности и доступности информации. Этим обосновывается **актуальность** проведенного исследования.

В диссертации поставлена и успешно решена **научная задача** по разработке и обоснованию научно-методического аппарата в области идентификации сетевых атак на беспроводные сенсорные сети с помощью анализа поведенческих характеристик сети. Построенная математическая модель профиля поведения сети в достаточной степени точно описывает поведение беспроводной сенсорной сети и приводит к удовлетворительным показателям точности идентификации. Предложенный метод на основе совместного использования нескольких классификаторов позволяет сократить длительность периода идентификации и количество анализируемых признаков. Методика идентификации атак на основе анализа поведения сети объединяет полученные научные результаты с разработанными компьютерными программами и позволяет повысить эффективность идентификации.

Достоверность экспериментальных данных обеспечивается использованием современных средств моделирования и анализа и в достаточной степени адекватной методики проведения исследования. Полученные в ходе экспериментов результаты соответствуют теоретическим положениям, выдвинутых соискателем.

Теоретическая и практическая значимость работы обосновывается возможностью дальнейшего развития области на основе полученных теоретических результатов и использования практических результатов и комплекса разработанных программных средств для проектирования систем обнаружения вторжений и программно-аппаратных устройств для проведения мониторинга сети и аттестации объектов автоматизации. Результаты, полученные в рамках исследования, апробированы на российских и международных конференциях, в текстах печатных изданий, в т.ч. журналах, рецензируемых ВАК.

Автореферат содержит формализованную постановку задачи, иллюстративный материал и в достаточной мере адекватно отражает содержание диссертационной работы.

По автореферату отмечены следующие замечания:

1. При описании метода идентификации не приведена информация о количестве записей в наборе данных, о соотношении обучающей и тестовой выборок и о сбалансированности данных.
2. В тексте автореферата упоминаются показатели эффективности идентификации, но не описано, какие это показатели и как присваиваются веса.

Отмеченные замечания в большей степени не влияют на качество работы и полученные результаты.

Диссертационная работа является научно-квалификационной работой, выполнена в соответствии пп. 9-14 «Положения о присуждении ученых степеней», утвержденного постановлением Российской Федерации от 24 сентября 2013 г. № 842. Соискатель Коржук Виктория Михайловна заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Должность профессор
доктор технических наук,
старший научный сотрудник

Виктор Григорьевич Швед

Дата: 03 декабря 2019 г.

Адрес: Санкт-Петербург, ул. Жукова, д. 18.

Тел.: (812) 612-12-36

Email: office@gkspr.ru