ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета Д.002.199.01 по кандидатской диссертации Дойниковой Елены Владимировны на тему: «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов», научный руководитель – д.т.н., профессор, заведующий лабораторией проблем компьютерной безопасности СПИИРАН Котенко И.В.

Экспертная комиссия диссертационного совета Д.002.199.01 в составе: д.т.н., проф. Молдовяна А.А. (председатель), д.т.н., проф. Воробьева В.И., д.т.н., проф. Осипова В.Ю. после ознакомления с кандидатской диссертацией Дойниковой Елены Владимировны сделала вывод о том, что диссертационная работа Дойниковой Е.В. посвящена решению актуальной научной и практической задачи: разработки модельно-методического аппарата для оценки защищенности компьютерных сетей и выбора защитных мер для систем мониторинга безопасности и управления инцидентами.

Целью исследования является повышение защищенности компьютерных сетей за счет усовершенствования методик, моделей и алгоритмов оценки защищенности и выбора защитных мер на основе вычисления показателей защищенности.

Выбор направления обусловлен тем, что не смотря на предпринимаемые усилия в области информационной безопасности, количество и сложность киберпреступлений продолжает расти. Перспективным подходом к проактивному реагированию на компьютерные атаки является постоянное отслеживание ситуации по защищенности на основе изменения значений разнообразных показателей для своевременной реализации рациональных защитных мер. Для сбора и обработки информации по безопасности предназначены системы мониторинга безопасности и управления инцидентами. Однако реализованные в них методики не позволяют получить всестороннюю оценку ситуации и рекомендации по выбору защитных мер на основе адекватных количественных показателей. Поэтому разработка комплексного подхода к оценке защищенности компьютерных сетей и выбору защитных мер, основанного на вычислении различных показателей защищенности и применимого для систем мониторинга безопасности и управления инцидентами является важной задачей данной предметной области.

Методологической и теоретической основой задачи являются научные работы отечественных и зарубежных авторов в областях управления информационной безопасностью, оценки защищенности, принятия решений, логико-вероятностного анализа, системного анализа, оптимизационного анализа, анализа уязвимостей программно-аппаратных систем, программной инженерии и проектирования.

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации обеспечивается тщательным анализом состояния исследований в области, подтверждается согласованностью результатов, полученных при экспериментах, успешной апробацией на ряде научных конференций всероссийского и международного уровня, и публикацией в ведущих рецензируемых научных изданиях.

Новизна полученных автором диссертационного исследования результатов заключается в разработке и формализации методик и алгоритмов оценки защищенности компьютерных сетей и выбора защитных мер на основе формирования адекватных количественных показателей при различных наборах входных данных и на различных уровнях функционирования системы, применимых для систем мониторинга безопасности и управления инцидентами.

Материалы и основные результаты кандидатской диссертации Дойниковой Е.В. удовлетворяют паспорту специальности: 05.13.19 – «Методы и системы защиты информации, информационная безопасность», по которой диссертационному совету Д.002.199.01 предоставлено право проведения защит диссертаций.

Основные научные результаты диссертации удовлетворяют требованиям, предусмотренным пунктами 11 и 13 Положения о присуждении ученых степеней: по

материалам диссертационной работы опубликовано более 40 научных работ, в том числе 33 статьи, из которых 9 статей в периодических журналах, рекомендованных ВАК (журналы «Информационно-управляющие системы», «Безопасность информационных технологий», «Проблемы информационной безопасности. Компьютерные системы», «Известия высших учебных заведений. Приборостроение», «Труды СПИИРАН»), 12 в зарубежных изданиях, входящих в систему цитирования Web of Science и Scopus.

Недостоверные сведения о работах, в которых изложены основные научные результаты диссертации, опубликованных соискателем ученой степени, отсутствуют.

Текст диссертации, представленной в диссертационный совет, идентичен тексту диссертации, размещенной на сайте СПИИРАН.

Объем оригинального текста диссертационной работы составляет не менее 90%; цитирование оформлено корректно. Требования, установленные пунктом 14 Положения о присуждении ученых степеней, соблюдены: заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем ученой степени в соавторстве, без ссылок на соавторов, не выявлено.

Комиссия предлагает:

1. Принять кандидатскую диссертацию Дойниковой Е.В. к защите на диссертационном совете Д.002.199.01 как соответствующую профилю диссертационного совета по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.
2. В качестве официальных оппонентов назначить специалистов по данной проблеме: д.т.н., проф. Новикова В.А., д.т.н., проф. Иванова А.Ю.
3. В качестве ведущей организации утвердить АО «Научно-исследовательский институт «Рубин».
4. Разрешить Дойниковой Е.В. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «25» мая 2017 г.