ПРЕДВАРИТЕЛЬНОЕ РАССМОТРЕНИЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Гайворонской Светланы Александровны

«Исследование методов обнаружения шеллкодов в высокоскоростных каналах передачи данных», представляемой на соискание учёной степени кандидата физико-математических наук по специальности 05.13.11 «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей». Работа выполнена на кафедре Автоматизации систем вычислительных комплексов факультета Вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова. Научный руководитель доктор физико-математических наук, член-корреспондент РАН, профессор Смелянский Руслан Леонидович.

Диссертация посвящена разработке и исследованию методов обнаружения шеллкодов – вредоносных исполнимых кодов, удаленно эксплуатирующих ошибки работы с памятью, в высокоскоростных каналах передаче данных. В работе получены следующие результаты:

1. Предложена модель распознавания специфических признаков объектов, в рамках которой разработан алгоритм распознавания шеллкодов, позволяющий покрыть все известные классы шеллкодов, снизить вычислительную сложность обнаружения шеллкодов, минимизировать количество ложных срабатываний.

2. На основе анализа существующих шеллкодов выделено множество их специфических признаков, что позволило построить полную классификацию этого вида вредоносного программного обеспечения.

3. Разработанные алгоритмы классификации были реализованы и апробированы в рамках экспериментальной системы Demorpheus на четырех наборах данных: на наборе эксплойтов, на легитимных программах, на случайных и мультимедийных данных. Система продемонстрировала практически нулевое число ложных срабатываний, высокое значение пропускной способности по сравнению с линейной комбинацией существующих аналогов.

Положения диссертации отражены в пяти публикациях (в т.ч. две в изданиях из списка ВАК), неоднократно докладывались на различных научных семинарах и конференциях.

По итогам рассмотрения комиссия предлагает утвердить следующее:

Содержание диссертации соответствует специальности 05.13.11.

Официальные оппоненты

Доктор физико-математических наук, зам. Генерального директора ФГУП Главного научно-исследовательского вычислительного центра ФНС России, Баранов Александр Павлович.

.

Кандидат физико-математических наук, доцент кафедры информационной безопасности МГИУ (Федеральное государственное бюджетное образовательное учреждение высшего профессиональное образования «Московский Государственный Индустриальный Университет») Бутакова Наталья Георгиевна.

Ведущая организация:

Федеральное государственное бюджетное учреждение науки Научно-исследовательский институт системных исследований Российской Академии Наук (НИИСИ РАН)

Председатель комиссии:

Члены комиссии: