О Т З Ы В

научного руководителя на диссертационную работу

Гайворонской Светланы Александровны

«Исследование методов обнаружения шеллкодов в высокоскоростных каналах передачи данных»,

представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Гайворонская С.А. (1988 г.р.) поступила на первый курс факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова в 2005 году и окончила его в 2010 году. С 2010 года по 2013 год Гайворонская С.А. проходила обучение в очной аспирантуре.

Перед диссертантом стояла задача исследовать новые подходы к обнаружению вредоносного исполнимого кода, эксплуатирующего ошибки работы с памятью (шеллкода), при его передаче по высокоскоростным каналам передачи данных.

Научная новизна проведенного исследования Гайворонской С.А. заключается в построении математической модели распознавания шеллкодов, в рамках которой конструктивно строиться оптимальное по сложности и качеству распознавания решение – распознаватель исследуемых объектов по наборам специфичных для шеллкодов признаков. В работе на основе проведенного исследования впервые предложена классификация шеллкодов, которая обеспечивает полноту покрытия известных образцов шеллкодов.

Практическая значимость представленной работы заключается в возможности использования экспериментально реализованной системы обнаружения шеллкодов в рамках систем обнаружения и предотвращения вторжений (IDS/IPS) для выявления и фильтрации шеллкодов различных классов на этапе их транспортировке по высокоскоростным каналам передачи данных. Разработанная система позволяет существенно снизить вычислительную нагрузку как на сетевое оборудование, так и на конечное устройство.

Гайворонская С.А. занимается проблемой, рассматриваемой в диссертационной работе, с первого года аспирантуры. Кроме разработанной и реализованной системы обнаружения шеллкодов, Гайворонская С.А. занималась исследованиями устойчивости методов обфускации виртуализацией, применяемых к вредоносному программному обеспечению, а так же обнаружением и фильтрацией вредоносной активности в облачных архитектурах.

Предложенный в работе С.А. Гайворонской подход к обнаружению вредоносного исполнимого кода открывает новые возможности для исследователей в сфере сетевой безопасности, позволяя избежать распространенного подхода создания и поиска сигнатур. Предлагаемый подход позволяет обнаруживать как известные, так и принципиально новые образцы шеллкодов.

Все результаты, представленные в работе, являются достоверными. Достоверность результатов обеспечивается теоретическим обоснованием и тщательным экспериментальным исследованием, которое продемонстрировало применимость предложенного решения к высокоскоростным каналам передаче данных, высокую точность обнаружения шеллкодов и низкую долю ложных срабатываний.

По своим творческим и деловым качествам Гайворонская С.А. является зрелым квалифицированным специалистом, способным самостоятельно решать наукоёмкие задачи и разрабатывать прикладные исследовательские проекты. Соискатель умело оперирует различными математическими методами исследований при решении поставленных в работе задач. Считаю, что Гайворонской С.А. проделана большая и полезная работа. Диссертация демонстрирует высокий уровень научных способностей диссертанта и его творческие возможности.

Гайворонская С.А. участвовала в выполнении 2 НИР по грантам РФФИ. Имеет 7 научных публикаций, из них 5 за последние 3 года. Результаты работ представлены на шести международных конференциях.

Гайворонская С.А. успешно прошла научную стажировку в Университете Аризоны осенью 2012 года. Целями стажировки были: исследование применимости методов обфускации виртуализации к различным видам вредоносного программного обеспечения, а так же устойчивость таких методов. Летом и осенью 2013 года Гайворонская С.А. успешно прошла стажировку в исследовательском подразделении компании Майкрософт в Рэдмонде. Целью стажировки являлось исследование методов обнаружения вредоносной активности в облачных архитектурах на примере облачного решения Windows Azure.

Гайворонская С.А. провела всестороннее исследование поставленной задачи. Все результаты, представленные в работе, получены автором лично.

Диссертационная работа полностью удовлетворяет требованиям ВАК к диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 (математическое и программное обеспечение вычислительных машин, комплексов и

компьютерных сетей), а ее автор – Гайворонская Светлана Александровна – заслуживает присуждения ей искомой ученой степени.

Научный руководитель:

Член-корр. РАН, профессор Смелянский Р.Л.

ПОДПИСЬ УДОСТОВЕРЯЮ
ВЕДУЩИЙ СПЕЦИАЛИСТ
ОТДЕЛА КАДРОВ Т.Г. КОВАЛЕНКО