О Т З Ы В

официального оппонента на диссертацию
Гайворонской Светланы Александровны
«Исследование методов обнаружения шеллкодов в высокоскоростных каналах передачи данных»,
представленную к защите на соискание ученой степени
кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Работа Гайворонской С.А. посвящена изучению проблемы обнаружения наборов вредоносных исполнимых инструкций, эксплуатирующих ошибки, возникающие при работе с памятью. Подобные наборы, называемые шеллкодами, составляют существенный процент крупных инцидентов, связанных с киберпреступностью за последние годы. Это обусловлено тем фактом, что многие программно-аппаратные системы, включающие модули на языках программирования C/C++, подвержены уязвимостям работы с памятью. Значимость подобных уязвимостей не снижается и вряд ли будет снижаться в ближайшие годы.

Исследовательские работы, посвященные изучению проблемы обнаружения подобных вредоносных инструкций, впервые появились в начале 2000-х годов, и их число продолжает расти. Однако полученные в результате методы обнаружения имеют существенные недостатки: в первую очередь, они не способны обнаруживать все известные на текущий момент образцы вредоносных наборов инструкций, а также наборов инструкций, замаскированных обфускациями; часть методов характеризуется значительным числом ошибочных срабатываний, что может негативно сказаться на работе пользователей; часть методов имеют высокую вычислительную сложность, что ставит под сомнение их применимость в современных высокоскоростных каналах передачи данных.

В диссертации ставится задача разработки метода обнаружения шеллкодов, максимально полно охватывающего известные образцы шеллкодов, а так же характеризующегося низкой долей ошибочных срабатываний и оптимального с точки зрения вычислительной сложности. Таким образом, актуальность работы Гайворонской С. А. не вызывает сомнений.

Общая характеристика работы. Диссертация состоит из введения, пяти глав, списка литературы. Объем основного текста диссертации содержит 118 страниц, список литературы содержит 112 наименований.

Введение содержит описание предметной области, а так же обоснование актуальности поставленной задачи.

В первой главе диссертационной работы описана математическая модель процесса распознавания типичных признаков объектов, которыми в данной работе выступают наборы вредоносных исполнимых инструкций, эксплуатирующих работу с памятью – шеллкоды. В рамках представленной модели автором ставится задача распознавания объектов – то есть задача классификации объекта при условии заданного ограниченного набора классов объектов. Автором формально доказано существование решения поставленной задачи в приведенной модели, а само решение описано и подробно исследовано. Стоит отметить, что предложенная автором математическая модель и решение задачи классификации объектов являются универсальными и могут быть применимы не только для задачи распознавания вредоносных инструкций, но так же и в ряде других областей.

Во второй и третьих главах автором показывается применимость предложенной математической модели к исследуемой проблеме.

В частности, во второй главе диссертационной работы приводится описание характерных признаков вредоносных наборов инструкций, на основе которых впервые проводится классификация таких наборов.

В третьей главе приведен обзор существующих решений поставленной задачи, в котором выявлены недостатки существующих подходов и обоснована необходимость применения предложенного автором метода.

Четвертая глава посвящена описанию прототипа, реализующего предложенный автором подход к решению задачи обнаружения вредоносных наборов инструкций. В данной главе так же приводится описание результатов апробации реализованного прототипа. Стоит отметить аккуратность проведенного исследования: использовались различные наборы данных, на основании которых сделано заключение о точности обнаружения вредоносных наборов инструкций в канале, доле ошибочных срабатываний прототипа, о скорости его работы, а так же о полноте обнаружения введенных автором классов наборов вредоносных исполнимых инструкций.

Материал диссертации представляет несомненный интерес для исследователей в области информационной безопасности.

Результаты работы Гайворонской С.А. имеют значительную научную и практическую ценность. С практической точки зрения, работа может быть использована в рамках как существующих систем обнаружения и предотвращения вторжений, а также быть самостоятельной экспериментальной системой обнаружения, превосходящей существующие аналоги, как по полноте обнаружения, так и по доле ложных срабатываний и скорости работы.

Диссертация хорошо оформлена и написана ясным языком.

По диссертации имеются следующие замечания:

1. Автором выбран формат построения диссертации, при котором непосредственный анализ существующих методов обнаружения шеллкодов содержится не в начале, а в третьей главе диссертации, т.е. не служит основой для построения собственной модели для метода обнаружения. Собственная же модель автора представлена уже в первой главе диссертации. Такой порядок изложения приводит к неопределенности в вопросе сравнения и пригодности рассматриваемых методов в высокоскоростных каналах передачи данных.
2. В классификации шеллкодов по способам маскирования (обфускации) не отражены криптографические методы защиты. В рассмотренных вредоносных исполнимых инструкциях сложные криптографические алгоритмы не могут быть применены. Однако простые криптографические методы защиты шеллкодов от обнаружения широко используются на практике, поэтому в работе стоило упомянуть об этих методах.
3. Последовательность ссылок библиографии диссертации не соответствует последовательности изложения материала. Так, например, первая ссылка имеет номер [95], вторая [48] и т.д.
4. В работе присутствует ряд орфографических и пунктуационных ошибок (например, на стр.9, на стр.99 и др.).

Указанные недостатки никоим образом не снижают в целом положительной оценки диссертации, которая, несомненно,

представляет собой законченное научное исследование, удовлетворяющее всем требованиям, предъявляемым 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. Главные положения, выдвинутые диссертантом, являются новыми научными результатами. Они опубликованы в 5 печатных работах, 2 из которых - в изданиях, рекомендованных ВАК, неоднократно обсуждались на российских и международных конференциях и получили одобрение ведущих специалистов. Автор, безусловно, заслуживает присуждения искомой степени.

Официальный оппонент,
доцент кафедры информационной
безопасности МГИУ,
кандидат физ.-мат. наук Н.Г.Бутакова

Подпись Бутаковой Н.Г.
Заверяю Д. Шленик
03.09.14