«УТВЕРЖДАЮ»
Заместитель директора НИИСИ РАН, д.т.н.

_____ Бобков С.Г.

«3» сентября 2014 г.

О Т З Ы В

ведущей организации (Научно-исследовательский институт системных исследований Российской Академии Наук НИИСИ РАН) о диссертации 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.

Диссертация Гайворонской С.А. посвящена изучению актуальной проблемы обнаружения вредоносного исполнимого кода, распространяющегося по высокоскоростным каналам передачи данных. Данная проблема представляет интерес для исследователей в области информационной безопасности, а так же для ряда других направлений, в которых встает задача распознавания объектов, то есть отнесения их к множеству наперед заданных классов. Соискатель ставит перед собой задачу распознавания шеллкодов в сетевом трафике на этапе их транспортировке по высокоскоростным каналам, что накладывает ряд ограничений на решение. В частности, из-за большого объема проходящего по высокоскоростным каналам трафика, решение должно удовлетворять требованиям по вычислительной сложности и доле ошибок. Кроме того, к решению предъявляются требования обнаружения всех известных на сегодняшний день типов шеллкодов.

Во введении настоящей работы сформулирована цель исследований и показана ее актуальность. Так же во введении описана предметная область, введены используемые в работе основные понятия.

В первой главе автор предлагает формальную математическую модель, включающую в себя ряд абстракций, позволяющих описать процесс отнесения объектов к множеству наперед заданных классов, а так же описывающую свойства этих объектов. В терминах предложенной математической модели формализована задача распознавания объектов, описано типичное решение этой задачи и указаны его недостатки. Соискателем предложено новое решение этой задачи, основная идея которого заключается в задании на множестве алгоритмов, вычисляющих значения признаков объектов, отношения частичного порядка, в соответствии с которым алгоритмы выстраиваются в некоторую структуру, определяющую порядок их выполнения. Идея выполнения алгоритмов в приведенной структуре заключается в следующем. Если в объекте некоторыми алгоритмами не были обнаружены соответствующие вычисляемые признаки, то объект не анализируется другими алгоритмами. Такой подход позволяет снизить суммарную вычислительную сложность решения. В тексте диссертации формально доказано, что предложенное решение задачи распознавания шеллкодов оптимизирует вычислительную сложность традиционных подходов к решению задачи, имеет гарантировано минимальную долю ложных срабатываний и способно обнаруживать образцы шеллкодов заданных классов, то есть обеспечивает полное покрытие классов шеллкодов.

Во второй главе настоящей работы подробно описаны типичные признаки шеллкодов, на основе которых автором предложена классификация существующих на данных момент шеллкодов. Стоит

отметить, что классификация представляет интерес сама по себе – в ней учтены как статические, так и динамические (поведенческие) характеристики исследуемых объектов. Так же в классификации нашли отражение типичные приемы «запутывания» программного кода, применяемого злоумышленниками. Для построения заданной классификации соискателем была проделана существенная аналитическая и техническая работа, включающая в себя анализ доступных исходных кодов вредоносных наборов инструкций и соответствующей литературы.

В третьей главе рассмотрены существующие методы обнаружения шеллкодов. Глава хорошо структурирована – методы обнаружения шеллкодов рассмотрены в соответствии с общепринятой классификацией. Приведен анализ этих методов с точки зрения их применимости к поиску шеллкодов в высокоскоростных каналах передачи данных, в результате которого показана их небольшая практическая значимость. В качестве вывода из данной главы автор обосновывает актуальность применения предложенного подхода к решаемой задаче.

Четвертая глава описывает архитектуру программного средства, реализующего решение, предложенного автором в первой главе. Программное средство способно обнаруживать типичные признаки шеллкодов, описанных во второй главе и проводить распознавание шеллкодов в соответствии с предложенной классификацией. Стоит отметить, что при описании программного средства, соискатель так же уделил внимание ряду интересных технических решений, применяемых им при реализации программного средства. В частности, описаны недостатки существующих подходов к дизассемблированию битовых строк (в частности, по скорости работы), приведено описание

и анализ алгоритма, применяемого автором для решения этой задачи. Так же в четвертой главе описана методика тестирования программного средства, описан и обоснован выбор наборов тестовых данных, приведены результаты тестирования. Программное средство является продуктом с открытым исходным кодом, все полученные результаты работы с программным средством воспроизводимы.

Все результаты, полученные автором в работе, являются новыми и вносят существенный вклад в развитие области информационной безопасности, опубликованы в ведущих научных журналах и обнародованы на ведущих международных конференциях. Научная составляющая диссертационной работы может найти свое применение не только в сфере информационной безопасности, но и в ряде других областей. Практическая реализация предложенного подхода уже нашла применение в ряде организаций.

Автореферат полностью отражает содержание диссертационной работы.

Тем не менее, по диссертации имеются следующие замечания:

1. Апробация программного средства не была проведена на реальных каналах передачи данных. Результаты экспериментальных исследований, приведенных в тексте диссертационной работы, основываются на синтетически сгенерированных данных, было бы интересно посмотреть результаты работы программного средства в «боевых» условиях.
2. В тексте работы отсутствует описание процесса установки программного средства на рабочую систему, в то время как это не очевидный процесс.
3. В тексте присутствует ряд несущественных погрешностей, которые носят характер описок.

Имеющиеся недостатки не влияют на содержательную сторону диссертационной работы и не ставят под сомнение основные ее результаты. Диссертация удовлетворяет требованиям «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации, а ее автор Гайворонская Светлана Александровна заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Заведующий отделом НИИСИ РАН,
к.ф.-м.н. Грюнталь А.И.