«УТВЕРЖДАЮ»

И.о. проректора по научной работе СПбГЭТУ

Д.В.Гайворонский

09 _____2017 г.

ОТЗЫВ

на автореферат диссертации Израилова Константина Евгеньевича
по теме «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных системах»
представленной на соискание учёной степени кандидата технических наук
по специальности - 05.13.19 - «Методы и системы защиты информации, информационная безопасность»

В автореферате диссертации Израилова К.Е. изложена суть проведённого исследования, посвящённого уязвимостям в программном обеспечении телекоммуникационных устройств. Всестороннее рассмотрение современного состояния теоретической и методологической базы показывает, что классические взгляды на способы поиска уязвимостей в исходном коде не удовлетворяют современным требованиям, поскольку преобладающее количество телекоммуникационных устройств поставляется с машинным кодом, способы поиска по которому существенно ограничены и в разы более трудоемки. В таких условиях применение стандартов общей практики приводит к постоянному нарушению верифицированного состояния сред облачных вычислений. Таким образом, на сегодня не имеется соответствующих необходимым требованиям средств реверс-инжиниринга. Учитывая основной принцип общей практики, определяемый нормативными документами данной отрасли, заключающийся в постоянном поддержании выполняемых мер безопасности, Израилов К.Е. задаёт основной целью исследования новый вид представления машинного кода, специализированный для поиска средне- и высокоуровневых уязвимостей, так называемое алгоритмизированное представление. При современном уровне востребованности технологий связи и телекоммуникации решение поставленной задачи, заключающейся в разработке новых подходов, учитывающих все факторы изменений таких систем, представляется крайне актуальной.

В автореферате хорошо показано, что недостаточно рассмотренной остаётся ситуация, складывающаяся в результате легитимных изменений в конструкции телекоммуникационных устройств, возникающих ввиду действий поставщика устройств, изменяющего функциональность сред без

участия пользователей, что приводит в разных случаях к неправильному функционированию системы поиска недекларируемых возможностей.

Помимо выделенных самим автором положений, выносимых на защиту, следует отдельно подчеркнуть несколько особенностей работы:

1. в работе всесторонне рассмотрены действующие методологические основы анализа уязвимостей телекоммуникационных систем, а приведённые автором модели непротиворечиво вписываются в правила общей практики, задаваемые рассматриваемой нормативной базой, выявляя при этом уязвимости, что позволяет повысить уровень защищённости;
2. в работе вводится понятие алгоритмизации машинного кода упрощающей работу аналитика.

Основой комплекса подходов, предлагаемых автором, являются хорошо разработанная архитектура программных средств алгоритмизации машинного кода, отличающаяся наличием иерархически-связанных структурных элементов – структурных метаданных и разноуровневых уязвимостей.

Необходимо выделить также несколько недостатков в тексте автореферата:

1. В работе некорректно используется методология поиска уязвимостей в машинном коде. В настоящее время более близкой методологией является поиск недекларируемых возможностей и использование анализаторов исходных текстов. Предлагаемые автором решения ближе к решению задач верификации ПО.
2. В автореферате нет полноценного сравнения предлагаемого решения с существующими, как зарубежными, так и отечественными. Для оценки потребительских свойств предлагаемой утилиты в качестве альтернативы выбран продукт IDA Pro с плагином декомпиляции Hex-Rays при наличии отечественного дизасемблера RD16 Л.Н. Афанасьева и разработок отечественных трансляторов программ с Ассемблера на языки высокого уровня.
3. В процессе дизассемблирования могут возникать ситуации, на которые заранее не могут быть написаны инструкции. Например, команды JMP и CALL могут иметь и неявную адресацию перехода\вызова. Эти адреса могут предварительно загружаться в регистры или размещаться в области данных в виде таблиц. В этих ситуациях уровня машинного декодирования явно недостаточно. Необходим переход на уровень смыслового декодирования, чтобы проанализировать, например, структуру таблицы.

Указанные недостатки никоим образом не снижают ценность работы, особенно учитывая глубину исследования и приведённые примеры формализации задачи исследования.

Таким образом, исследование соответствует требованиям, предъявляемым к диссертациям на соискание учёной степени кандидата наук п. 9 Положения о присуждении учёных степеней, утверждённого постановлением Правительства РФ от 24.09.2013 № 842, а Израилов К.Е.

заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Заведующий кафедрой «Информационная безопасность»
Санкт-Петербургского государственного электротехнического
университета «ЛЭТИ» им. В.И. Ульянова (Ленина),

ктн, доцент Воробьев Евгений Германович

Наши реквизиты: Федеральное государственное автономное образовательное учреждение высшего профессионального образования “Санкт-Петербургский государственный электротехнический университет “ЛЭТИ” им. В.И. Ульянова (Ленина)” (СПбГЭТУ) Минобрнауки России, юр.адрес: ул. Проф. Попова, 5, С.-Петербург, 197376, Тел.: (812) 346-44-87, факс: (812) 346-27-58, E- mail: eltech@eltech.ru.