АО «СИСТЕМЫ УПРАВЛЕНИЯ»

Акционерное общество

«Научно-производственное объединение «Импульс»

(АО «НПО «Импульс»)

Киришская ул., 2, лит.А, Санкт – Петербург,195299
Тел./Факс (812) 290-48-55,
Телеграф БАРК, А/Т 321205
E-mail: kanz@npoimpuls.ru
http: www.npoimpuls.ru
ОГРН 1127847076202
ИНН/КПП 7804478424/780401001

11 СЕН 2017 № 110/4677

УТВЕРЖДАЮ

Первый заместитель генерального директора – главный конструктор

Заслуженный деятель науки РФ доктор технических наук, профессор

С.М. Доценко

сентября 2017 г.

ОТЗЫВ

на автореферат диссертационной работы Израилова Константина Евгеньевича на тему «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Зависимость информационной безопасности отдельной личности, общества и всего государства от используемых инфокоммуникационных сетей привела к актуализации целого ряда угроз, связанных с использованием небезопасного телекоммуникационного оборудования. Предпосылки к последнему заключаются в вынужденном использовании устройств, программное обеспечение которых является проприетарным и наиболее подверженным наличию скрыто внедренных уязвимостей, таких, как программные закладки. Имеющийся арсенал средств автоматического поиска применим лишь для тривиальных уязвимостей в случае точного задания соответствующих правил; последнее труднореализуемо для более «комплексных» уязвимостей уровня алгоритмов и архитектуры программного обеспечения, создаваемых при этом вручную. Отсутствие же исходного кода такого программного обеспечения и недостаточная развитость области реверс-инжиниринга не позволяют на сегодняшний день эффективно осуществлять их ручной поиск.

Вышеизложенное предопределило актуальность темы диссертационного исследования, проведенного Израиловым К.Е. и посвященного способу получения высокоуровневых архитектуры и алгоритмов программного обеспечения из низкоуровневого представления – машинного кода, функционирующего в телекоммуникационном оборудовании.

Автором предполагается гипотеза о наличии в машинном кода метаданных, содержащих информацию о структурных элементов различного уровня абстракции, таких, как архитектура кода, его деление на модули, входящие в них подпрограммы с входными и выходными параметрами, алгоритмы с условными переходами и логикой вычислений. Рассмотрение программного обеспечения на каждом таком уровне позволяет выявлять собственный набор уязвимостей различных типов, а именно низко-, средне- и высокоуровневых. Обоснование гипотезы делается как с теоретической точки зрения, так и путем практической демонстрации с помощью разработанного прототипа программы алгоритмизации.

Судя по автореферату, соискателю удалось справиться с целями и задачами, поставленными в диссертации. В ходе проведенного исследования автором получены следующие основные научные результаты, выносимые на защиту:

1) Структурная модель машинного кода с уязвимостями;
2) Метод алгоритмизации машинного кода;
3) Архитектура программного средства алгоритмизации машинного кода;
4) Комплекс научно-методических средств оценки алгоритмизации машинного кода в интересах поиска уязвимостей.

Новизна основных научных результатов обеспечивается тем, что автором по-новому рассматривается машинный код – с точки зрения восстановления его алгоритмов работы, в результате чего созданы оригинальные метод и программное средство алгоритмизации; последние используют собственную модель машинного кода, отличную от классической учетом структурных элементов кода и их иерархических связей. Также, для оценки алгоритмизации предназначается авторский комплекс научно-методических средств, состоящий из целого ряда методик и критериев.

Достоверность и обоснованность научных положений диссертации обеспечивается использованием широкого круга научно-методических и научно-технических источников, обстоятельным теоретическим анализом предметной области, применением апробированных методов исследования и подтверждается результатами тестирования, а также зарегистрированным свидетельством на программу для ЭВМ.

Вместе с тем, по автореферату можно высказать отдельные замечания:

1) В тексте автореферата нет пояснения, что понимается в работе под термином «блок машинного кода».
2) Отсутствует обоснование выбора критериев Метода Анализа Иерархий (МАИ).
3) Из реферата не ясно, как соотносится введенная классификация {НУ, СУ, ВУ} со стандартной классификацией, указанной в ГОСТ 56 546-216.

Высказанные замечания не носят принципиального характера. Автореферат убеждает в том, что диссертация Израилова К.Е., выполненная с учетом современного уровня общенаучных и специальных знаний, является самостоятельным, завершенным научным исследованием, в котором содержится решение задачи, имеющей существенное значение для информационной безопасности телекоммуникаций.

Анализ автореферата позволяет сделать вывод, что диссертация Израилова К.Е. на тему «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах» полностью соответствует требованиям, предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения

ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв подготовлен помощником главного конструктора кандидатом технических наук Шаблюком Станиславом Марковичем и начальником научно-технического центра кандидатом технических наук Филипповым Сергеем Владимировичем.

Отзыв на автореферат диссертационной работы Израилова К.Е. рассмотрен на НТС НПО «Импульс» 08.09.2017, протокол № 6.

Помощником главного конструктора
кандидат технических наук

Шаблюк Станислав Маркович

Начальник научно-технического центра
кандидат технических наук

Филиппов Сергей Владимирович