ОТЗЫВ

на автореферат диссертации Гибилинды Романа Владимировича на тему «Разработка автоматизированных методов анализа воздействий на файлы в задаче расследования инцидентов информационной безопасности», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Расследование инцидентов информационной безопасности (ИБ) позволяет выявить уязвимости в системе обеспечения ИБ и сформировать рекомендации по их устранению. Известны несколько методов и средств, направленных на анализ различных данных с целью выявления воздействий на информацию, хранимую в файлах, фиксации активности вредоносных программ и др. Вместе с тем, в процессе анализа специалист сталкивается рядом проблем: это отсутствие механизма верификации обрабатываемых данных, отсутствие единого набора признаков, по которым возможно определение различных воздействий, в том числе на файлы. Поэтому возникает потребность в разработке новых математически обоснованных методов и моделей для анализа данных.

В работе получен ряд новых научных результатов, в том числе: разработана событийная модель процесса идентификации воздействий на файлы; разработан кластеризационный метод идентификации воздействий на файлы; разработан метод экспресс-анализа событий ИБ, связанных с воздействиями на файлы.

Обоснованность научных положений диссертации следует из корректной постановки задач исследования и результатов экспериментальной апробации предложенных моделей и методов.

Основные результаты исследования опубликованы в шести научных работах, три из которых в ведущих рецензируемых журналах, рекомендованных ВАК РФ, одна – в цитатно-аналитической базе Scopus. Получены два свидетельства о регистрации программ для ЭВМ.

Вместе с этим, следует отметить некоторые замечания и вопросы по содержанию автореферата:

1. В тексте автореферата не приведены преимущества разработанного алгоритма автоматического подбора параметров кластеризации в сравнении с известными алгоритмами.

2. На рисунке 3 не указан накопитель файловых операций δ, являющийся одним из основных параметров представленной модели.

Сделанные замечания носят дискуссионный характер и не снижают научной ценности рецензируемой по автореферату работы.

Диссертационная работа изложена современным научно-техническим языком, она в полной мере отвечает требованиям к актуальности, практической значимости, научной новизне, отражению результатов в публикациях, а также полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ и специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Автор диссертации Гибилинда Роман Владимирович заслуживает присуждения ему учёной степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Доктор физико-математических наук, профессор,
профессор кафедры радиофизики и радиоэлектроники
физического факультета ФГБОУ ВО "Иркутский государственный университет",
664003, Российская Федерация, г. Иркутск, ул. К.Маркса, 1,
телефон (3952) 521900, e-mail: rector@isu.ru
Корольков Юрий Дмитриевич

18.10.2021

Контактные данные:
телефон +79996416620, e-mail: korol1@mailserv.isu.ru

Отзыв д-ф-м.н., профессора
Ю.Д. Королькова заверяю:
Ученый секретарь ФГБОУ ВО «ИГУ»
Кузьмина

ФГБОУ ВО «ИГУ»
ПОДПИСЬ УДОСТОВЕРЯЮ
Специалист по кадрам
М.П. Забелина
«18» 10 2021 г.