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) является неотъемлемой частью процедуры усиления мер защиты информации. Идентификация воздействий на файлы в рамках расследования инцидента позволяет оценить и ликвидировать последствия. Существующие методы и средства позволяют лишь частично выявлять факты нарушения трех основных критериев безопасности информации (конфиденциальности, целостности и доступности), хранимой в файлах. Вместе с тем, помимо воздействий на пользовательскую информацию также необходимо определять факты запуска стороннего программного обеспечения (ПО), в том числе вредоносного, в обход действующей политики безопасности, внесения изменений в конфигурационные файлы средств защиты и операционной системы и т.д. Дополнительно следует отметить, что достоверность данных, по которым проводится анализ во время расследования, зачастую требует проверки. В связи с этим разработка новых методов анализа воздействий на файлы является актуальной задачей.

В работе получен ряд новых научных результатов, в том числе: разработана модель процесса идентификации воздействий на файлы, позволяющая формализовать набор признаков, характеризующих файл; разработан кластеризационный метод идентификации воздействий на файлы; разработан метод экспресс-анализа событий ИБ, позволяющий сократить время на обнаружение и классификацию воздействий.

Практическая значимость заключается в создании комплекса программных средств, обеспечивающего автоматизацию процесса анализа воздействий на файлы в рамках расследования инцидентов ИБ и в разработке рекомендаций по совместному использованию комплекса с существующим ПО.

Обоснованность и достоверность научных результатов исследования достигнута благодаря корректной постановке цели исследования, корректному выбору математического аппарата задачам исследования и результатами экспериментальной апробации предложенных моделей и методов анализа воздействий на файлы.

Результаты исследования опубликованы в 6 научных работах, 3 из которых в ведущих рецензируемых журналах, рекомендованных ВАК РФ. Присутствуют

2 свидетельства о регистрации программ для ЭВМ.

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

1. В тексте автореферата на странице 11 введен признак Z_f, но нет пояснений о его назначении и каким образом он связан с компонентами вектора V_f.

2. Отсутствует описание принципа работы алгоритма № 1 кластеризационного метода идентификации воздействий на файлы, в результате чего не удается однозначно определить взаимосвязь между алгоритмами № 1 и № 2. Графические пояснения, приведенные на рисунках 4 и 5 также не способствуют корректному восприятию информации.

3. На рисунке 5 точки описаны координатами ($T_{m,f}$, $U_{m,f}$), а в выражении (4) используются ($T'_{m,f}$, $U'_{m,f}$), описание которых не приведено в тексте автореферата. Равны ли указанные значения?

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

Исследовательская работа изложена грамотным научно-техническим языком, в полной мере отвечает требованиям по 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.

Кандидат юридических наук
доцент кафедры финансового мониторинга (№ 75)
Института финансовых технологий и экономической безопасности
Национального исследовательского ядерного университета «МИФИ»
Тел.: +7-999-983-44-62
e-mail: ibnorms@gmail.com
Адрес организации: 115409, Российская Федерация, г. Москва, Каширское шоссе, д. 31

Фадеев Михаил Михайлович _____

21 октября 2021 г.

ПОДПИСЬ ЗАВЕРЯЮ
ЗАМ. ДИРЕКТОРА ПО
ПЕРСОНАЛУ НИЯУ МИФИ
Л. В. ВАСИЛЕНКО

ДИРЕКЦИЯ ПО УПРАВЛЕНИЮ ПЕРСОНАЛОМ