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. Существует несколько методов и средств, направленных на анализ различных данных (оперативной памяти компьютера, накопителей информации, пользовательских и системных файлов и т.д.) с целью определения хода инцидента. Так возможно выявлять воздействия на информацию, хранимую в файлах, фиксировать активность компьютерных вирусов, а также обнаруживать попытки несанкционированного доступа к информации. Вместе с тем, в процессе анализа специалист сталкивается рядом проблем: отсутствие механизма верификации обрабатываемых данных, отсутствие единого набора признаков, по которым возможно определение различных воздействий в т.ч. на файлы. 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 результатов исследования достигнута благодаря корректной постановке задач исследования и результатом экспериментальной апробации предложенных моделей и методов.

Результаты исследования опубликованы в 6 научных работах, 3 из которых в ведущих рецензируемых журналах, рекомендованных ВАК РФ, 1 – в цитатно-аналитической базе Scopus. Получены 2 свидетельства о регистрации программ для ЭВМ.

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

1. В тексте автореферата не указано соотношение между величинами t (момент времени при котором зафиксированы значения признаков, характеризующих файлов) и T_f (время появления записи о действиях над файлом в журнале $UsnJrnl). Указанный недостаток не позволяет дать однозначный ответ о времени фиксации промежуточных

состояний файла *f*.

2. На стр. 9 указано, что существующие процедуры автоматического подбора оптимальных параметров кластеризации имеют недостатки, но не приведен перечень этих процедур, в результате чего становится непонятно, с чем автор сравнивает предложенный им алгоритм. Также не указаны преимущества разработанного алгоритма в сравнении с существующими.

3. Отсутствует описание принципа работы алгоритма № 3 кластеризационного метода идентификации воздействий на файлы, что затрудняет корректное восприятие результатов работа метода в целом.

4. В заключении указаны перспективы дальнейшего исследования с указанием о возможности доработки созданного комплекса программных средств, которая является не научной, а инженерной задачей.

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.

Доцент базовой кафедры № 252 – информационной безопасности
Института кибернетики МИРЭА – Российского технологического университета
кандидат технических наук, доцент
Тимаков Алексей Анатольевич
Тел.: +7(985) 114 11 71
e-mail: timakov@mirea.ru

Адрес организации:
119454, ЦФО, г. Москва, Проспект Вернадского, д. 78

18.10.2021 г.