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

Вследствие осуществления компьютерных атак на информационные системы организации специалисты по обеспечению информационной безопасности (ИБ) должны проводить расследования возникающих инцидентов ИБ. Одним из ключевых моментов расследования является определение воздействий на информацию и ликвидация последствий этих воздействий. Существующие методы и средства позволяют лишь частично выявлять факты нарушения конфиденциальности и/или целостности информации, хранимой в файлах, определять запуск стороннего программного обеспечения (ПО) в обход действующей политики безопасности, обнаруживать попытки внесения изменений в конфигурацию в т.ч. систем обеспечения ИБ. Дополнительно следует отметить, что данные, на основе которых проводится анализ во время расследования, зачастую требуют дополнительной 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, и осуществить проверку данных, полученных из массива данных операционной системы; разработан метод идентификации воздействий на файлы посредством кластерного анализа, что уменьшает временные затраты на идентификацию воздействий; разработан метод экспресс-анализа событий ИБ, связанных с воздействиями на файлы, позволяющий сократить время на обнаружение и классификацию воздействий.

Практическая значимость заключается в разработке комплекса программных средств, обеспечивающего автоматизацию процесса анализа воздействий на файлы, а также в создании рекомендаций по совместному использованию комплекса с существующим ПО, применяемым при расследовании инцидентов ИБ.

Обоснованность и достоверность научных результатов исследования достигнута благодаря корректной постановке цели и задач исследования, адекватному 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 нет пояснений, что означает элемент «Вызов исключения» блок-схемы, представленной на рисунке 2, из-за чего принцип работы алгоритма становится «непрозрачен».

2. В тексте автореферата не указан критерий, по которому алгоритм № 3 кластеризационного метода идентификации воздействий на файлы «осуществляет поиск сложных комплексных воздействий». Без текста диссертационной работы об основе алгоритма можно лишь догадываться.

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.

Богданов Валентин Викторович

к.т.н.
Генеральный директор
ООО «Уральский центр систем безопасности»
Тел.: +7 (343) 379-98-34, доп. 1101
e-mail: vbogdanov@ussc.ru
Адрес организации: 620100, г. Екатеринбург, ул. Ткачей, д. 6

21.10.21

(подпись) (дата)

М.П.

Подпись Богданова В.В. заверяю

Л.С. КАРТЬЯНОВА
/ДОВ. №143 ОТ 28.05.2021/