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 совершенствования мер по защите информации. Определение воздействий на информацию является важным этапом расследования, позволяющим 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 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, связанных с воздействиями на файлы, 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 нет указаний о том, по каким критериям следует создавать шаблоны воздействий на файлы и наполнять ими базу данных. Проверялась ли актуальность и адекватность созданных шаблонов на других компьютерах с тем же типом операционной системы?

2. На рисунке 10 изображен модуль «генератор компьютерных атак», но нет пояснений, какое программное или программно-аппаратное обеспечение может быть использовано в качестве этого модуля. Допускают ли разработанные методы осуществление воздействий на файлы «вручную» в целях генерации шаблонов без использования указанного модуля?

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.

Полякова Елена Николаевна

кандидат педагогических наук, доцент
директор института математики и интеллектуальных систем,
ФГБОУ ВО «Курганский государственный университет»
Тел.: 89128320200
e-mail: penelena1972@yandex.ru
Адрес организации:

640020, г. Курган, ул.Советская, 63, стр. 4

14.10.2021

(подпись) (дата)

М.П.

ВЕРНО
Зав. канцелярией
Козлова М.А.
«15» 10 2021 г.