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

Осуществление компьютерных атак на информационные системы государства приводят к возникновению инцидентов, которые негативно влияют на экономическую, социально-политическую и промышленные сферы жизнедеятельности общества. В целях противодействия подобным инцидентам в будущем проводится их расследование. Одним из этапов расследования является определение воздействий на информацию, хранимую в файлах. Несмотря на то, что существует несколько работ отечественных и зарубежных ученых, посвященных анализу массивов данных с целью определения воздействий на файлы, проблемы поиска внесенных искажений в данные, а также отсутствия единого формализованного набора признаков, по изменению которых можно однозначно определить воздействия, по-прежнему возникают в процессе расследования инцидента. 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 верификацию данных, полученных из массива; разработан кластеризационный метод, используемый для создания шаблонов воздействий; разработан метод экспресс-анализа событий ИБ, связанных с воздействиями на файлы, использующий ранее подготовленные шаблоны и 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. Издана 1 статья в журнале, индексируемом в международной цитатно-аналитической базе Scopus Присутствуют 2 свидетельства о регистрации программ для ЭВМ.

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

1. На стр. 8 автореферата перечислены признаки, характеризующие файл, которые являются компонентами вектора $V_j(t)$, но нет пояснений, почему выбран именно такой набор компонент. В связи с этим возникает вопрос о полноте множества приведенных типов файловых операций.

2. На рисунке 3, где изображена событийная модель идентификации воздействий на файлы в виде сети Петри, отсутствует накопитель файловых операций δ, который является неотъемлемой частью представленной модели.

3. Из текста автореферата не понятно, какой закон распределения плотности вероятности может быть использован в формуле (4) для расчета длины описания $L(x)$.

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.

Доктор технических наук, доцент
Заместитель генерального директора по НТР – главный конструктор
АО «Уральское производственное предприятие «Вектор» (АО «УПП «Вектор»)

Пономарев Олег Павлович _____ 28.10.2021

Контактные данные: тел. 8-982-6041745, e-mail: ponomarev7713@mail.ru

Адрес места работы:
620078, Российская Федерация, г. Екатеринбург, ул. Гагарина, 28, АО «Уральское производственное предприятие «Вектор».

Подпись сотрудника Пономарева О.П. заверяю:
Начальник отдела кадров АО «УПП «Вектор» _____ Еременко Владислав Ильич