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

Процесс расследования инцидентов информационной безопасности (ИБ) неразрывно связан с анализом множества массивов данных, которые имеют разнородную структуру и содержат различный объем информации. К таким массивам относят журналы событий операционной системы, журналы файловой системы, сведения о последних открывавшихся файлах, информация о запущенных процессах в образе оперативной памяти компьютера и т.д. Использование существующих методов и средств анализа данных позволяет ограниченно выявлять воздействия на информацию, хранимую в файлах, фиксировать активность вредоносного программного обеспечения, а также обнаруживать попытки обхода действующей политики безопасности с целью получения несанкционированного доступа к информации. Дополнительно следует отметить, что достоверность данных, по которым проводится анализ во время расследования, зачастую требует проверки. В этой связи разработка новых методов анализа воздействий на файлы является актуальной задачей.

В работе получен ряд новых научных результатов, в том числе: разработана событийная модель процесса идентификации воздействий на файлы, позволяющая осуществить верификацию данных, полученных из массива; разработан кластеризационный метод идентификации воздействий на файлы, используемый для создания шаблонов 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 при расследовании инцидентов ИБ.

Обоснованность и достоверность научных результатов исследования достигнута благодаря корректной постановке задач 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. На рисунке 7 видно, что признак N_f при создании шаблона разделяется на четыре компонента, изображенные в виде части таблицы. Каждый компонент назван одинаково – N_G. В тексте автореферата не хватает пояснений, почему в представленной на рисунке таблице столбцы имеют различные наименования, а компоненты именуются идентично.

2. На рисунке 9 нетрудно заметить, что введенные т.н. «дополнительные условия аномальности» включают в себя значения времени/даты и некие «расположения». Из текста автореферата не понятно «расположения» чего должны быть указаны в качестве условий аномальности.

3. Достоверны ли записи журнала изменений тома $UsnJrnl в случае расследования инцидента на высоконагруженных файловыми операциями системах в условиях конкурентного доступа процессов к носителю информации с файлом журнала?

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.

Гильмияров Роман Владимирович

Генеральный директор
ООО «Институт радиоэлектронных систем»
Тел.: +7 (343) 374-24-64
e-mail: zi@irsural.ru
Адрес организации: 620137, г. Екатеринбург, ул. Июльская, д. 41

28.10.2023

(подпись) (дата)

М.П.

Подпись генерального дире
заверяю,
Заместитель генерального д
Сюндюков И.Э.