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 занимает важную роль в определении и ликвидации последствий осуществленных на автоматизированные системы управления технологическими процессами компьютерных атак. Процесс расследования предполагает анализ множества массивов данных, которые имеют разнородную структуру и не всегда пригодны к осуществлению «ручного» анализа. Использование существующих методов и средств анализа данных позволяет ограниченно фиксировать активность вредоносного программного обеспечения, а также выявлять воздействия на информацию, хранимую в файлах. Также следует отметить, что достоверность данных, по которым проводится анализ во время расследования, может быть подвержена сомнению, если злоумышленник попытался «замести следы». 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.

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 1 видно, что автор приводит различные массивы данных с информацией о воздействиях на файлы, которые могут быть проанализированы в ходе расследования инцидента. Объем данных в некоторых массивах составляет, согласно рисунка, десятки записей, что вполне может быть проанализировано «вручную». Требуется ли автоматизация анализа в данном случае?

2. На рисунке 2 отсутствует операция «чтения» содержимого файла. В связи с чем она была исключена из рассмотрения?

3. В тексте автореферата не пояснены вопросы оптимизации временных затрат при поиске минимального значения $L(x)$. Требуется ли рассчитывать значение $L(x)$ для всех k, или первое полученное значение, которое больше предыдущего, говорит о том, что глобальный минимум достигнут?

Сделанные замечания имеют дискуссионный характер и не снижают научной ценности рецензируемой по автореферату работы.

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.

Даю согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета, и дальнейшую их обработку

Заведующий кафедрой
«Автоматизация технологических процессов»
Березниковского филиала ФГБОУ ВО
«Пермский национальный исследовательский
политехнический университет»
профессор, д.т.н. по спец. 05.13.01 А.В. Затонский

/21.10.2021

Затонский Андрей Владимирович, 618404, Пермский край,
г. Березники, ул. Тельмана, 7, 8(3424)26-90-90, zxenon@narod.ru