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

Определение воздействий на информацию является значимой процедурой в рамках расследования инцидента информационной безопасности (ИБ). Существующие методы и средства позволяют лишь частично выявлять факты воздействия на хранимую в файлах информацию. Вместе с тем, объемы обрабатываемой в ходе расследования информации, а также применение аналитическим методов «вручную» не всегда позволяют быстро локализовать и ликвидировать последствия инцидента. Также следует отметить, что достоверность данных, по которым проводится обработка и анализ во время расследования, зачастую требует проверки. В связи с этим разработка новых автоматизированных методов анализа воздействий на информацию, хранящуюся в файлах, 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 точной постановке цели исследования, корректному соответствию математического аппарата задачам исследования, 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. Соискатель представил 2 свидетельства о регистрации программ для ЭВМ.

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

автореферата:

1. Отсутствует описание параметра $G_{priority}$. В чем заключается его назначение?

2. На рисунке 7 изображен шаблон сложного воздействия на файл, причем параметр N_G одновременно отмечен как значимый, так и незначимый в разных полях шаблона. С чем связано такое определение значимости полей шаблона?

3. На рисунке 10 указан элемент А3 «Генератор компьютерных атак», но не дано его описание.

4. Используются метрики Precision и Recall без указания для какого класса они были вычислены. Обычно эти метрики указываются отдельно для каждого класса, или только для самого значимого класса.

5. В тексте употребляется F-score и F-мера. Возникает вопрос, это одна и та же, или разные метрики? Более корректно для метрики использовать F1-score вместо F-score.

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.

ФИО:

Кандидат физико-математических наук, доцент
Заведующий кафедрой компьютерной безопасности и прикладной алгебры
Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет»
Тел.: +7 (351) 799-72-92
e-mail: csukbcp2011@gmail.com
Адрес: 454001, г. Челябинск, ул. Братьев Кашириных, 129

18.10.2021

Ручай Алексей Николаевич

Подпись Ручай А.Н.
удостоверяю