ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора физико-математических наук, профессора Титова Сергея Сергеевича на диссертационную работу 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

Актуальность темы исследования

По требованиям нормативных актов в случае возникновения в информационной системе (ИС) непредвиденной ситуации, направленной на нарушение действующей политики безопасности необходимо проводить расследование инцидентов информационной безопасности (ИБ), чтобы определить недостатки системы обеспечения ИБ и устранить последствия инцидента. При расследовании инцидентов зачастую возникает потребность в определении воздействий на информацию. Архитектура используемых файловых и операционных систем подразумевает использование файлов для хранения информации. Таким образом, процесс определения воздействий на информацию может быть сведен к обнаружению и классификации воздействий на файлы. Основой для определения воздействий являются данные, содержащиеся в разноструктурированных массивах, которые могут содержать важную для расследования информацию. «Ручной» анализ возможен в случае небольшого объема данных (десятки-сотни элементов массива), но при росте количества записей до десятков-сотен тысяч (например, в случае обработки данных нескольких компьютерах из состава ИС) неизбежно приводит увеличению сроков расследования. Решением возникшей проблемы является автоматизация процесса обнаружения и классификации воздействий файлы, которая частично рассматривалась в нескольких работах. Тем не менее, в созданных автоматизированных методах определения воздействий на файлы существуют несколько не разрешенных вопросов: потребность в нормализации данных из нескольких массивов; отсутствие возможности автоматического подбора оптимальных параметров анализа; необходимость в проверке данных массива на предмет наличия искажений.

В этой связи разработка новых методов автоматизированного определения воздействий на файлы является актуальной задачей.

Научная новизна полученных результатов

В диссертационной работе получены следующие новые научные результаты:

- разработана модель процесса идентификации воздействий на файлы,

позволяющая формализовать набор признаков, характеризующих файл, и осуществить проверку данных, полученных из массива;

• разработан кластеризационный метод идентификации воздействий на файлы, направленных, в том числе, на нарушение действующей политики ИБ, используемый для уменьшения временных затрат на идентификацию воздействий;

• разработан метод экспресс-анализа событий ИБ, связанных с воздействиями на файлы, основанный на использовании ранее подготовленных в рамках кластеризационного метода шаблонов, позволяющий сократить временные затраты на обнаружение и классификацию воздействий.

Практическая значимость результатов диссертации

Практическая значимость заключается в разработке комплекса программных средств, обеспечивающего автоматизацию процесса анализа воздействий на файлы, в том числе направленных на нарушение действующей политики ИБ. Полученные результаты внедрены в ООО «Уральский центр систем безопасности» (Екатеринбург, Россия); в ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина» (Екатеринбург, Россия); в ОКБ «Новатор» (Екатеринбург, Россия).

Обоснованность и достоверность научных положений, сформулированных в диссертации

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, 4 из которых в ведущих рецензируемых журналах, рекомендованных ВАК РФ и Аттестационным советом УрФУ. Присутствует 2 свидетельства о регистрации программ для ЭВМ.

Оценка содержания и оформления диссертации

Диссертационная работа содержит 178 страниц, из них 139 – основного текста, 16 рисунков (без приложений) и 16 таблиц (без приложений). Структурно работа состоит из введения, трех глав, заключения, списка сокращений и условных обозначений, списка литературы, включающего 151 наименование и 5 приложений.

Первая глава посвящена рассмотрению состояния предметной области, в тексте приведен обзор результатов, полученных в работах отечественных и зарубежных учёных. Автором комплексно рассмотрел проблему анализа данных о воздействиях на файлы, в том числе направленных на нарушение действующей политики ИБ, при расследовании

инцидентов. После ввода определений, лежащих в основе дальнейшего исследования, автор описывает существующие массивы данных и методы их анализа. Выбор кластерного анализа как наиболее подходящего метода обосновано возможностью сокращения объема обрабатываемой информации при оптимальном подборе параметров разбиения данных массива. Для решения проблемы достоверности анализируемых данных автор рассматривает распространенные схемы моделирования и обосновывает выбор математического аппарата сетей Петри. В конце главы автор формулирует цель и задачи исследования на основе анализа состояния предметной области.

Вторая глава состоит из трех частей. Первая описывает разработку событийной модели идентификации воздействий на файлы, которая может использоваться для проверки анализируемых данных на предмет наличия искажений. В тексте приведены условия использования модели и интерпретация получаемых результатов. Во второй и третьей частях автор предлагает методы, применяемые во взаимосвязи и предназначенные для сокращения временных затрат на анализ данных в процессе расследования инцидента ИБ. Кластеризационный метод идентификации воздействий на файлы позволяет автоматизировать процедуру определения составляющих воздействия. Автором продемонстрировано, что предварительное разделение данных на блоки и автоматический подбор необходимых параметров кластеризации с использованием принципа «минимальной длины описания» позволяет получить оптимальное разбиение на кластеры, описывающие воздействия. Полученные кластеры используются для создания шаблонов, являющихся декомпозицей данных о воздействии на файл, которая содержит только значимые и постоянные критерии обнаружения и классификации воздействий на компьютере, где произошел инцидент ИБ. Созданные шаблоны сохраняются в виде базы данных, которая используется в предложенном автором методе экспресс-анализа событий ИБ, связанных с воздействиями на файлы. Применение шаблонов позволило получить гибкий механизм классификации с возможностью быстрого изменения/добавления необходимых классов воздействий, а также сократить временные затраты на проведение классификации.

В третьей главе диссертации описан процесс разработки и использования комплекса программных средств, реализующих предложенные во второй главе событийную модель и методы. Взаимосвязи между элементами комплекса наглядно представлены IDEF0-схемами. В тексте приведены рекомендации в части предварительной подготовке эталонного массива данных, содержащих информацию о воздействиях на файлы, а также по использованию комплекса для достижения наилучшего результата анализа воздействий на файлы. В тексте приведен сравнительный анализ созданных математических методов кластеризации и классификации с другими, широко

применяемыми при анализе массивов данных. Полученные результаты оцениваются с посредством расчета коэффициентов точности, полноты и *F*-меры. Показано, что предложенные методы не уступают существующим исходя из значений рассчитанных коэффициентов, но обладают преимуществами, которые найдут свое применение на практике. Рассмотрены примеры совместного использования разработанного комплекса программных средств и существующего программного обеспечения, применяемого при расследовании инцидентов ИБ.

Замечания и вопросы по работе

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

1. В тексте автореферата нет пояснений, что означает элемент «Вызов исключения» блок-схемы, представленной на рисунке 2. Без текста диссертации принцип работы алгоритма остается неясен.

2. Алгоритм № 2 кластеризационного метода идентификации воздействий на файлы, представленный в п. 2.2.3 диссертации, предполагает использование некоторого конечного набора функций плотности распределения вероятности, но не дано обоснование, почему выбраны именно эти функции.

3. В п. 2.2.6, где описан порядок применения кластеризационного метода идентификации воздействий на файлы, утверждается, что метод универсален при выполнении нескольких условий, предъявляемых к входным данным. Была ли осуществлена проверка выдвинутого предположения в отношении других типов журналов?

4. В п. 2.3.2 описан алгоритм обнаружения и классификации воздействий на файлы с применением базы данных шаблонов, в котором используются векторы коэффициентов. Компоненты векторов имеют вес равный 1. Возникали ли ситуации, когда необходимо указывать вес отличный от единицы?

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

Заключение по работе

Исследовательская работа изложена грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, практической значимости, научной новизне, личному вкладу автора, 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.

Официальный оппонент:

Доктор физико-математических наук, профессор
Главный научный сотрудник кафедры «Информационные технологии и защита информации»
ФГБОУ ВО «Уральский государственный университет путей сообщения»
Тел.: +7 (343) 221-24-04
e-mail: stitov@usurt.ru
Адрес: 620034, г. Екатеринбург, ул. Колмогорова, д. 66

Титов Сергей Сергеевич

_____ 26.10.2021
(подпись) (дата)

Подпись Титова С.С. заверяю

Специалист по кадрам _____ М.А. Кондрашкина