ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук, доцента Соколова Александра Николаевича 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

Согласно требованиям нормативных актов, владельцы информационных систем (ИС) обязаны применять меры по защите информации, обрабатываемой и хранимой на компьютерах и устройствах, составляющих ИС, в том числе проводить расследование инцидентов информационной безопасности (ИБ).

Результаты расследования позволяют определить недостатки системы обеспечения ИБ и являются основанием для усиления принятых мер по защите информации. Процесс расследования состоит из нескольких этапов, в ходе которых анализируется различная информация: данные энергонезависимой памяти компьютера, журналы событий, сетевые соединения, содержимое машинных носителей с целью обнаружения и классификации воздействий на хранимую в файлах информацию. Основой для определения воздействий являются данные, содержащиеся в разноформатных массивах, которые могут содержать десятки-сотни тысяч записей / полей / иных различных информационных структур. Анализ в «ручном» режиме указанного объема данных неизбежно приводит к ошибкам, связанным с «человеческим фактором» и увеличению сроков проведения расследования инцидента. Следует отметить, что решения задачи автоматизации процесса обнаружения и классификации воздействий на информацию, хранимую в файлах, в целях сокращения сроков проведения расследования, частично рассматривались несколькими авторами. Были предложены алгоритмы кластеризации данных, представленных в виде совокупности признаков, представлены методы анализа на основе существующих алгоритмов классификации данных. Вместе с тем, отдельную сложность для создания автоматизированных методов определения воздействий на файлы представляют:

- отсутствие в массивах данных единого формализованного набора признаков, по порядку изменения которых возможно определить воздействия на файлы;

- потребность в автоматизированном подборе оптимальных параметров анализа данных с обоснованием критериев оценки;

• необходимость подтверждения достоверности анализируемых данных в целях своевременного выявления в них 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, для их последующего анализа в рамках расследования инцидентов ИБ;

• разработан кластеризационный метод идентификации воздействий на файлы, направленных, в том числе, на нарушение действующей политики ИБ, используемый для создания шаблонов воздействий;

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

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.

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).

Оценка содержания диссертации и её оформления

Диссертационная работа содержит 139 страниц основного текста (всего 178 с.), 16 рисунков (без приложений) и 16 таблиц (без приложений). Состоит из введения, трех глав, заключения, списка сокращений и условных обозначений, списка литературы из 151 наименования, 5 приложений.

В первой главе подробно рассмотрено состояние предметной области, сделан акцент на результатах, полученных как в работах отечественных, так и зарубежных учёных. Автор систематизировано и последовательно ведет свое исследование, рассматривая 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 рассматривает существующие массивы данных и методы их анализа. Приведено обоснование выбора кластерного анализа как наиболее подходящего метода в рамках решаемой задачи. Для решения проблемы достоверности анализируемых данных автор рассматривает типовые модели и обосновывает выбор математического аппарата сетей Петри, используемого при описании как последовательных, так и параллельных процессов с дискретным характером изменения параметров, присущим процессу осуществления воздействия на файл. Здесь же на основе анализа состояния предметной области автор формулирует цель и задачи исследования.

Вторая глава посвящена разработке событийной модели идентификации воздействий на файлы, которая может использоваться для верификации (подтверждения достоверности) анализируемых данных. В целях сокращения временных затрат на анализ данных в процессе расследования инцидента автор предлагает два метода. Кластеризационный метод идентификации воздействий на файлы направлен на автоматизацию процедуры определения составных частей каждого воздействия на файл. Показано, что предварительная подготовка входных данных и автоматическое определение оптимальных параметров кластеризации с использованием принципа «минимальной длины описания» позволяет получить кластеры данных, каждый из которых описывает осуществленное воздействие на файл. Полученные кластеры используются для создания шаблонов воздействий – декомпозиции данных о воздействии на файл, которая содержит только значимые и постоянные критерии поиска воздействий на компьютере, где произошел инцидент ИБ. Шаблоны хранятся в базе данных, которая используется в предложенном автором методе экспресс-анализа событий ИБ, связанных с воздействиями на файлы. Применение шаблонов воздействий позволило отказаться от ресурсоемких и времязатратных процедур по подбору оптимальных параметров классификации в пользу

определения воздействий в массиве данных путем простого порогового сравнения.

Третья глава исследования посвящена разработке комплекса программных средств, реализующих предложенные во второй главе модель и методы. Описание функциональных связей комплекса наглядно представлено в виде IDEF0-схем. В тексте приведены рекомендации по использованию комплекса для достижения наилучшего результата анализа воздействий на файлы. Проводится сравнительный анализ выбранных математических алгоритмов кластеризации и классификации с другими, применяемыми при анализе массивов данных. Полученные результаты оцениваются с использованием коэффициентов точности и полноты. Рассмотрены примеры совместного использования разработанного комплекса программных средств и существующих программных решений, применяемых при расследовании инцидентов ИБ.

Замечания и вопросы по работе

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

1. Исходя из заданных границ исследования (с. 6 автореферата и с. 11 и 63 диссертации), следует полагать, что автор ограничился лишь семейством операционных систем (ОС) Windows (Windows 7 Professional SP1, Microsoft Windows 8.1 Professional, Microsoft Windows 10 Professional) с файловой системой NTFS и журналом изменений тома $UsnJrnl. В связи с этим возникают вопросы:

– насколько актуальными могут быть представленные исследования для распространенных в настоящее время ОС Linux, СУБД Oracle и т.д.?

– из рис. 1 автореферата (с. 4) и рис. 1.1 диссертации (с. 5) не ясно, используются ли представленные массивы данных, содержащие информацию о воздействиях на файлы, во всех существующих операционных системах, или рассмотрен лишь конкретный пример?

– из текста автореферата (с. 11) и разд. 2.2 диссертации (с. 75) следует, что выносимый на защиту кластеризационный метод идентификации воздействий на файлы применен только к одному журналу $UsnJrnl. Можно ли распространить этот метод и на другие журналы событий? Если да, то на какие?

2. На с. 6 автореферата и с. 8 диссертации при формулировке п.3 научной новизны работы сказано, что разработан метод экспресс-анализа событий ИБ, связанных с воздействиями на файлы, позволяющий ускорить процесс обнаружения и классификации воздействий. Можно ли привести примеры СЗИ и средств обеспечения ИБ, где мог бы использоваться разработанный метод экспресс-анализа?

3. В разделе 1.6 (с. 58) диссертации перечислены программные средства, применяемые при расследовании инцидентов ИБ. Может ли представленное исследование улучшить характеристики, например, известного сертифицированного отечественного программно-аппаратного комплекса для автоматического выявления инцидентов на основе анализа событий ИБ ViPNet TIAS (Threat Intelligence Analytics System) и в какой части?

4. Зависимость $\Psi = g(\tau, K_f)$, описываемая формулой (9) на с. 76 диссертации, охарактеризована как возрастающая и нелинейная, но также указано, что существуют ограничения по значению величины $U_f \in \Psi$. Актуально ли описывать зависимость как возрастающую по достижению максимального значения U_f ? В тексте диссертации не рассмотрена подобная ситуация.

5. В табл. 2.4 (с. 83) диссертации рассмотрены известные распределения непрерывных случайных величин, которые используются в алгоритмах кластеризации. В связи с этим возникают вопросы:

– математическое ожидание нормального распределения обозначено через μ. В то же время при рассмотрении сетей Петри параметр μ имеет другой смысл (на с. 58 диссертации μ – это маркировка). Логичней было бы для математического ожидания использовать другое обозначение (например, букву a)?

– в тексте после табл. 2.4 сказано, что «достаточно использовать PDF нормального или гамма-распределения с оптимальными значениями параметров, указанными в табл. 2.4, при расчете значения $L(x_m, c)$ для определения оптимального количества кластеров k». На основании каких данных сделан такой вывод?

6. В разделе 2.3.1 (с. 91) диссертации сказано, что представленный метод экспресс-анализа событий, связанных с воздействиями на файлы, включает процесс генерации шаблонов воздействий на файлы, который использует процедуры экспертной оценки и определяется специалистом-аналитиком, подготавливающим шаблон (признаки аномальности, приоритета и значимости). Существуют ли рекомендации для значений этих параметров?

7. На с. 96 диссертации сделан вывод о том, что для хранения результатов вычислений оптимальным выглядит выбор метрики Левенштейна. На основании чего сделан этот вывод?

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, научной новизне, практической значимости, 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:

Кандидат технических наук, доцент
Заведующий кафедрой «Защита информации» Высшей школы электроники и компьютерных наук
ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)»
Тел.: +7 (351) 267-93-55
e-mail: sokolovan@susu.ru
Адрес: 454080, г. Челябинск, просп. Ленина, д.87, ауд. 907, 911/3бв

29.10.2021

Соколов Александр Николаевич

ись) (дата)

Подпись Соколова А.И. удостоверяю
Начальник управления по работе с кадрами Н.С. Минакова

Управление по работе с кадрами