АО «АСТ»
115230, г. Москва, Каширское шоссе, д.3, корпус 2, стр.4
109316, г. Москва, Остаповский проезд, д.3, стр.26
+7 (495) 679-86-86
hello@acti.ru

Advanced System Technologies
www.acti.ru

ОТЗЫВ

на автореферат диссертации Пантюхина Игоря Сергеевича
по теме «Методика и методы обеспечения аудита средств вычислительной техники для расследования компьютерных инцидентов»,
представленной на соискание учёной степени кандидата технических наук
по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

В работе И.С. Пантюхина рассматривается проблема управления инцидентами безопасности СВТ в условиях ограниченного времени исследования. Отмечается специфический характер проводимых компьютерно-технических экспертиз (КТЭ), заключающийся в недостаточной степени покрытия выявляемых обнаружений и формирования цифровых улик с последующим расследованием и реконфигурации СЗИ для предотвращения инцидентов в дальнейшем. Автором исследуется спектр вопросов, связанных с анализом атрибутов данных и их особенностями применения для различного окружения в т.ч. памяти, сетевого трафика и т.п. При этом комплексируются известные методы обработки данных для расширения степени покрытия исходных данных и учитывается характер связей между наборами данных.

Соискатель убедительно показывает неприменимость либо ограничения во многих случаях известных методов и необходимости доработки и разработки, новых связанных с определением атрибутов и учёта связи событий. Эти параметры учитывают функциональные особенности программных компонент рассматриваемых сред и в отдельных случаях естественным образом опираются на отраслевые особенности. Предложенные методы реализованы программно и опробованы на широко известных решениях, что также подтверждается свидетельствами о регистрации программы для ЭВМ и актами внедрения.

К новым и оригинальным результатам можно отнести:

1. Действенная методика для получения атрибутов в условиях ограниченного временного интервала что позволяет оптимизировать затраты на КТЭ без её снижения ниже необходимого уровня.

2. Комплексирование нескольких методов проведения пост-инцидентного аудита СВТ с применением теории графов, что позволяет реконструировать взаимосвязи между набором данных и событий для произошедших инцидентов.

В то же время, можно отметить некоторые недостатки, связанные с апробацией, не снижающие значения проделанной автором работы и весомость полученных результатов. Рассмотрение проблемы проведения пост-инцидентного аудита на основе графов для описания взаимосвязей с одной стороны выглядит неочевидным с точки зрения масштабирования, например, при применении в средах контейнеризации, с другой – неявно предполагает расширение результатов в плоскости профилирования инцидентов с учётом общих признаков окружения и должно было быть более подробно описано, так как представляет отдельный интерес и направление для последующей разработки и интеграции с сопряжёнными информационными системами.

В целом, диссертационная работа соответствует требованиям, предъявляемым к кандидатским диссертациям, а её автор, И.С. Пантюхин заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6 - Методы и системы защиты информации, информационная безопасность.

Ю.С. Чемёркин, к.т.н., ведущий специалист

Подпись Чемёркина Ю.С. заверяю
руководитель Управления исследований и
разработки, АО «АСТ»
к.т.н, М.В. Левыкин
17.01.2023

Чемёркин Юрий Сергеевич,
к.т.н., ведущий специалист Управления исследований и разработки
АО «АСТ»
109316, Россия, Москва, Остаповский проезд, 3, строение 26
E-mail: y.chemerkin@acti.ru