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.

Работа Пантюхина И.С. посвящена развитию методов и методик обеспечения аудита средств вычислительной техники для расследования компьютерных инцидентов. В настоящее время сложность и количество кибератак с каждым годом увеличивается экспоненциально. Как следствие, возникает необходимость разработки новых методов выявления и предотвращения компьютерных инцидентов. Важной составляющей является аудит средств вычислительной техники для сбора и последующего анализа данных с дампов памяти. Одним из ключевых параметров в данном процессе является время, необходимое для проведения анализа. Именно поэтому разработка методов аудита средств СВТ, направленных на уменьшение времени получения информативных данных, набирает все большую популярность как в науке, так и в индустрии. Таким образом, можно сделать вывод, что тема диссертационной работы Пантюхина И.С. актуальна.

В результате исследования соискателем предложены:

1. Методика проведения постинцидентного внутреннего аудита средств вычислительной техники для получения максимально-доступного количества данных с последующим представлением информации в виде атрибутов и их значений.
2. Метод проведения постинцидентного внутреннего аудита средств вычислительной техники на основе графов для описания взаимосвязей между атрибутами и их значениями.
3. Метод снижения объема обрабатываемой информации за счет классификации пользовательских и системных данных. .

При изучении работы были выявлены следующие замечания и недостатки:

1. В работе автор говорит об постинцидентном аудите, который, обычно проводится «посмертно», после обнаружения инцидента. В этом контексте очевидна целесообразность анализа различных дампов. Однако, автор не поясняет, как можно проводить анализ сетевого трафика, если инцидент уже заершен и никакого трафика уже нет.

2. Работа имеет ярко выраженную практическую направленность. В связи с этим хотелось бы видеть не только абсолютные оценки полученных результатов, но и сравнение с использованием других методов постинцидентного аудита на данных, полученных в результате одних и тех же инцидентов.

3. Разработанные в работе методы и методики имеют сугубо инженерный характер, что повлияло на представление самой работы и автореферата. В свете вышесказанного, представляется, что в работе следовало бы более четко сформулировать научную ценность и научную новизну полученных результатов.

Отмеченные замечания, однако, не носят значительный характер и не уменьшают научной и практической ценности полученных результатов, как и общего положительного впечатления о работе.

Научно-квалификационная работа Пантюхина И.С. на тему «Методика и методы обеспечения аудита средств вычислительной техники для расследования компьютерных инцидентов» является законченной работой, вносящей определенный вклад в теорию и практику. Тема, содержание и научные положения диссертационной работы Пантюхина И.С. соответствуют паспорту специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность. Все основные результаты работы опубликованы в рецензируемых научных журналах. Диссертационная работа по своему содержанию, научному уровню и завершенности исследований соответствует всем требованиям ВАК Российской Федерации, а ее автор, Пантюхин Игорь Сергеевич, заслуживает присвоения ученой степени кандидата технических наук по специальности 2.3.6 - Методы и системы защиты информации, информационная безопасность.

Директор Высшей школы интеллектуальных систем и суперкомпьютерных технологий,
кандидат технических наук, доцент

[redacted] Ицыксон Владимир Михайлович

195251, Санкт-Петербург, Политехническая ул., 29
Санкт-Петербургский политехнический университет Петра Великого
Тел: +7 (812) 775-05-30. Сайт http://spbstu.ru.

[redacted]