ОТЗЫВ

Бурлова Вячеслава Георгиевича

на автореферат диссертационной работы

Пантюхина Игоря Сергеевича

на тему «**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.

Активное развитие области кибербезопасности, а именно направления компьютерной криминалистики объективно требует разработки решений для повышения эффективности расследования компьютерных инцидентов. Диссертационная работа И.С. Пантюхина посвящена актуальной теме по разработке методики и методов сокращения временных затрат при расследовании компьютерных инцидентов. Современные кибератаки очень сложны, а их поиск затруднен в достаточно больших объемах данных на устройствах, подверженных действию кибератак.

Обеспечение аудита средств вычислительной техники - наиболее приоритетная задача при выполнении компьютерных экспертиз, а непосредственно анализ дампов памяти позволяет определить, была ли проведена атака и какой ущерб она нанесла. От качества и полноты дампа памяти зависит успешность проведенного аудита и обнаружение цифровой улики для дальнейшего расследования. В диссертационной работе для повышения скорости исследования компьютерных инцидентов автором предлагается анализ атрибутов и их значений, полученных с энергонезависимой, энергозависимой памяти и сетевого трафика.

К новым научным результатам можно отнести:

1. Методика проведения постинцидентного внутреннего аудита СВТ для получения максимально-доступного количества данных с последующим представлением информации в виде атрибутов и их значений.

2. Метод проведения постинцидентного внутреннего аудита СВТ на основе графов для описания взаимосвязей между атрибутами и их значениями.

3. Метод снижения объема обрабатываемой информации за счет классификации пользовательских и системных данных.

Предложенные соискателем методика и методы учитывают особенности современных аспектов кибербезопасности и были протестированы путем внедрения в практику компаний, чем подтверждена их применимость.

По тексту автореферата были отмечены следующие замечания:

1. Не ясно, как методы восстановления данных, применяемые в методике, позволяют достичь расширения признакового пространства для исследования компьютерных инцидентов.
2. В результатах эксперимента по тексту автореферата не указан тип энергонезависимой памяти, который участвовал в экспериментах, что улучшило бы общее восприятие результатов.

Отмеченные замечания не являются критическими и не снижают общей положительной оценки работы. Диссертация является законченной, научно-квалификационной работой, в которой присутствует научная и практическая ценность.

Диссертационная работа И.С. Пантюхина 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.

ИО заведующего кафедрой Информационных технологий
и Систем безопасности Российского государственного
гидрометеорологического университета
доктор технических наук [redacted] В.Г. Бурлов

24.01.2025

Организация: ФГБОУ ВО «РГГМУ».
Почтовый адрес: 192007, Россия, Санкт-Петербург, ул. Воронежская, дом 79.
Телефон: +7 812 633 01 82 Сайт: www.rshu.ru E-mail: rector@rshu.ru

[redacted]

Подпись Бурлова В.Г. заверяю
Нач. управления кадров [redacted] Кабова Л.В.