

УДК: 004

Название: Разработка метода оценки эффективности мероприятий по постинцидентному анализу.

Авторы: Безручко Ярослав Олегович (Университет ИТМО, Санкт-Петербург), Бейсова Аделина Хасиетуллаевна (Университет ИТМО, Санкт-Петербург), Феофилактов Николай Андреевич (Университет ИТМО, Санкт-Петербург).

Научный руководитель: Кузнецов Александр Юрьевич (Университет ИТМО, Санкт-Петербург)

Введение

Инциденты информационной безопасности происходят постоянно, имеют разные масштабы и последствия. Для того чтобы предотвратить повторение подобных инцидентов в будущем, необходимо должным образом проводить их расследование, выяснять вопросы, касающиеся их природы, повлекших их причин, влияющих на них факторов, а также разрабатывать тактику, направленную на их избежание.

В сфере информационной безопасности существует немало методов постинцидентного анализа, но к сожалению, универсального среди них нет. Поэтому для каждого конкретного случая разные методы по-разному эффективны. Чтобы избежать неоправданных потерь ресурсов нужно определить, какие методы постинцидентного анализа системы информационной безопасности будут наиболее эффективны.

Актуальность:

В открытых источниках отсутствует какая-либо информация о существовании методов оценки эффективности мероприятий по постинцидентному анализу, поэтому разработка такого метода является актуальной задачей.

Цель:

Целью работы является качественная оценка эффективности мероприятий по постинцидентному анализу, помогающая объективно и в адекватные сроки определить самый подходящий метод для заданных условий для наиболее рационального использования ресурсов организации и достижения результата за минимально возможный промежуток времени.

Объект исследования:

Чтобы должным образом оценить эффективность, нужно учесть основополагающие факторы, влияющие на процесс метода и его результат. Таким образом, объектом исследования является влияние различных факторов на эффективность методов постинцидентного анализа.

Общие сведения:

В работе раскрываются понятия количественных и качественных показателей эффективности, рассматриваются виды шкал, чтобы определить наиболее логичный подход к процессу оценки эффективности. Произведены обзор и классификация методов анализа, а также анализ факторов, влияющих на эффективность мероприятий по постинцидентному анализу. На основе проанализированных данных была оценена степень влияния различных параметров на оценку эффективности, а также выявлены взаимосвязи между ними. Выставлены требования, которым должен соответствовать разработанный метод.

Результаты:

В результате произведенной работы был получен метод, позволяющий получить качественную оценку эффективности мероприятий по постинцидентному анализу, включающий:

1. Формулу расчета эффективности мероприятий по постинцидентному анализу.
2. Таблицу, определяющую значения переменных, используемых в формуле, для рассматриваемого случая.
3. Методические указания.

Авторы: Безручко Я.О., +7 (921) 5637852, yar@milkmushrooms.com
Бейсова А.Х.
Феофилактов Н.А.

Научный руководитель: Кузнецов А.Ю.