

**ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ  
ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК  
В КОРПОРАТИВНЫХ СЕТЯХ**

Е.А. Мурашко, С.Н. Петров

Современные способы обнаружения и предотвращения сетевых атак с использованием программно-аппаратных средств защиты информации (СЗИ) широко распространены в сфере

информационных технологий. При этом процессы и методы испытаний зачастую засекречены. Данный факт объясняется тем, что в ситуации, когда описание процесса испытаний продукта находится в общем доступе, потенциальный злоумышленник может видеть места, через которые легче всего если не полностью перехватить информацию, то нанести ей вред. Обнаружение сетевых атак с использованием программно-аппаратных СЗИ способствуют своевременному обнаружению проблем, которые могут привести к успешным противозаконным действиям со стороны злоумышленника. Другими словами, заблаговременное обнаружение уязвимостей позволяет разработчикам технических и программных продуктов заблокировать все возможные варианты незаконных действий злоумышленника для получения выгоды. Для успешного применения программно-аппаратного СЗИ необходимо произвести его тестирование на соответствующем оборудовании и средствах соединения через каналы связи, соответствующих определенным требованиям и с использованием специализированного программного обеспечения. Результаты тестирования помогают увидеть, какими функциональными возможностями может обладать устройство, либо программный продукт, что позволит потенциальному покупателю, увидев заключения экспертов, определить, какое именно решение правильное и выгоднее всего использовать в организации сетевой инфраструктуры компании либо предприятия. Также определенные средства защиты информации возможно протестировать только лишь на определенном типе тестового стенда, содержащим в себе специфические элементы сетевой инфраструктуры.

### **Литература**

1. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН. – 2016. – Вып. 45. – С. 207–244.
2. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. – СПб: Питер, 2017. – 256 с.