

## ОТЗЫВ

официального оппонента Приорова Андрея Леонидовича на диссертацию Дарахма Ислама «Защита банковских компьютерных сетей от несанкционированного доступа в Палестине», представленную на соискание ученой степени кандидата технических наук по специальности 05.12.13 Системы, сети и устройства телекоммуникаций.

### 1. Актуальность темы

Диссертация посвящена актуальной задаче – исследованиям по защите банковских компьютерных сетей Палестины. Для достижения наибольшей эффективности защиты корпоративной информационно-телекоммуникационной сети (КИТС) необходимо защищать информацию в соответствии с ее ценностью в корпорации (в банке). Такая ситуация приводит к растущим затратам на компенсацию действия угроз безопасности информации КИТС и информационные технологии. Поэтому важно оптимизировать эти затраты и улучшать эффективность защиты.

Сложное и разветвленное оборудование КИТС, большой объем поступающей информации и различные несанкционированные информационные проникновения создают трудности в обеспечении нормальной работы банковских сетей. Указанные проблемы осложняют применение только традиционных математических методов, в том числе методов математической статистики, а также классических методов оптимизации сетевых структур для решения прикладных задач защиты информации в КИТС.

### 2. Содержание работы

Диссертация состоит из введения, 3 глав, заключения, списка литературы из 110 наименований, списка сокращений и приложений.

**Во введении** показаны проблемы телекоммуникационных сетей Палестины, обоснована актуальность работы и поставлены задачи, которые необходимо решить для улучшения защиты КИТС банковского сектора.

**В первой главе** рассматривается несанкционированный доступ к информации в банковских сетях Палестины, особенности технических каналов банковских корпоративных сетей по несанкционированному доступу и защите от него. Кроме того, рассмотрены особенности банковских сетей Палестины и обеспечение их информационной защиты.

**Во второй главе** предлагается структурная схема комплексной интеллектуальной системы поддержки принятия решений (СППР), которая содержит множество функциональных компонент, позволяющих диагностировать состояния КИТС, идентифицировать атаки и максимально автоматизировать и ускорить выработку управляющих воздействий при изменении ситуации в КИТС.

**В третьей главе** предложен алгоритм минимизации количества маршрутизаторов в сети, который позволил сократить в 3 раза время проектирования структуры сети и в 2 раза их число. Кроме того, разработаны математические модели знаний на основе нечеткой логики и алгоритма интеллектуальной СППР о структуре сети и принципах поиска информационных проникновений в задачах по защите информации в корпоративной сети. Кроме того, предложена модель для защиты информации в сети, которая может использоваться при ограниченных сведениях о ней. Такая ситуация характерна для банковских сетей Палестины.

По каждой главе и работе в целом сделаны аргументированные выводы.

Содержание автореферата в достаточной степени отражает основные положения диссертации.

### **3. Оценка новизны и достоверности**

В качестве основных научных результатов, полученных в диссертации, можно отметить следующее:

1. Предложена методика управления информационной безопасностью КИТС в условиях атак злоумышленников, использующая интеллектуальные нечеткие модели.
2. Предложен новый подход к нечеткому структурно-логическому обобщению

