

## **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

знаний на основе нечеткой интерпретации данных и знаний.

3. Разработаны методика структурной минимизации и методика идентификации при запросах доступа к ресурсам КИТС.

4. Разработан комплекс методик, программ и структур, позволяющий реализовать интеллектуальную систему поддержки принятия решений в задачах по защите информации в КИТС, использующий нечеткую логику.

Научные положения, выводы, практические результаты и рекомендации подтверждены корректным обоснованием и анализом концептуальных и математических моделей рассматриваемых способов управления информационной безопасностью и защитой информации в КИТС; наглядной технической интерпретацией моделей; данными экспериментальных исследований.

По теме диссертации опубликовано 9 печатных работ, из них 3 статьи в рецензируемых изданиях из перечня ВАК. Указанные публикации достаточно полно отражают полученные автором результаты.

#### **4. Практическая ценность работы**

заключается в том, что

- разработанные и предложенные модели, структуры и алгоритмы могут быть использованы при разработке, эксплуатации и реконструкции современных КИТС в Палестине;
- алгоритмы доведены до рабочих программ и позволяют решать достаточно широкий круг научно-технических задач. Разработана математическая модель действий злоумышленника по реализации им своих целей в системе вычислительных средств защищаемой КИТС, позволяющая оценивать качество функционирования системы защиты информации;
- разработки позволили уменьшить время проектирования сетей с маршрутизаторами в 3 раза, число маршрутизаторов в 2 раза, повысить эффективность защиты более чем на 70 %.

Полученные результаты исследований, разработанные алгоритмы и методики

внедрены на заводе «Электроприбор» (г. Москва) и в НПО «РИК» (г. Владимир). Кроме того, после защиты планируется внедрение результатов диссертационной работы в Палестине.

## **5. Замечания по диссертационной работе**

1. Отсутствуют сведения об аппаратуре и программном обеспечении, используемых в банковских телекоммуникационных сетях Палестины.
2. Не приведены сравнения с другими методами защиты информации в компьютерных сетях Палестины.
3. Отсутствует название банка, о котором идет речь в работе.
4. В библиографическом списке указано мало литературных источников по особенностям телекоммуникаций в Палестине.
5. На титульном листе диссертации отсутствует название и номер специальности, по которой защищается соискатель.
6. В диссертации и в автореферате указано различное количество публикаций соискателя, выполненных по тематике работы (в диссертации – 10, в автореферате – 9) и различное количество таблиц (в диссертации – 53, в автореферате – 33).
7. В автореферате мало рисунков (всего 3) и отсутствуют таблицы, что затрудняет восприятие материала, хотя в тексте диссертации их достаточно много.
8. Отсутствует подпись к рис. 3 автореферата, хотя к рис. 1, рис. 2 подписи есть.
9. В тексте диссертации и автореферата содержатся орфографические и пунктуационные ошибки.

Отмеченные замечания существенным образом не влияют на общую положительную оценку основных теоретических и практических результатов диссертации.

## **6. Заключение**

Диссертация Дарахма Ислама «Защита банковских компьютерных сетей от несанкционированного доступа в Палестине» является законченной научно-квалификационной работой, в рамках которой решается важная и актуальная

научно-техническая задача по защите информации от несанкционированного доступа в соответствующем классе сетей связи. Её основные научные и практические результаты соответствуют паспорту специальности 05.12.13 Системы, сети и устройства телекоммуникаций.

Рассматриваемая диссертационная работа удовлетворяет критериям, установленным Положением о присуждении ученых степеней, а её автор Дарахма Ислам заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 Системы, сети и устройства телекоммуникаций.

Официальный оппонент,  
доктор технических наук, доцент,  
Ярославский государственный университет им. П.Г. Демидова,  
доцент кафедры динамики электронных систем

  
Приоров Андрей Леонидович

Дата: 27.02.2015

150000, г. Ярославль, ул. Советская, д. 14

Телефон: 8-(4852)-79-77-75

E-mail: andcat@yandex.ru

Подпись д.т.н., доц. А.Л. Приорова заверяю:

Начальник управления по работе

с персоналом ЯрГУ





Р.И. Волкова

