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

Актуальность работы

Учитывая тенденцию к созданию единого информационного пространства и, как следствие, подключения корпоративных сетей к глобальной сети Интернет, следует ожидать атак на такие системы с целью их разрушения или получения коммерческой выгоды. Для достижения наибольшей эффективности защиты корпоративной информационно-телекоммуникационной сети (КИТС) необходимо защищать информацию в соответствии с её ценностью для корпорации (в данном случае - для банка).

Актуальность работы связана с необходимостью:

- разработки методики принятия решения о структуре КИТС и принципов поиска информационных проникновений на основе экспертной исходной информации и применения нечеткой логики (лингвистический подход),
- обеспечения комплекса современных средств защиты информации с идентификацией пользователей при запросах на доступ в КИТС.

Всё это особенно важно для Палестины, где глобальные и корпоративные сети находится в стадии становления и подвергаются вредоносным воздействиям соседних стран.

Содержание работы

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

В первой главе рассматривается несанкционированный доступ к информации в банковских сетях Палестины, особенности технических каналов (использование телефонных каналов и проводных и сотовых и различных сочетаний маршрутизаторов) банковских корпоративных сетей по несанкционированному доступу и защите от него. Рассмотрены особенности банковских сетей Палестины и обеспечение их информационной защиты.

Во второй главе предлагается структурная схема комплексной интеллектуальной системы поддержки принятия решений, которая содержит множество функци-

ональных компонент, позволяющих диагностировать состояния КИТС, идентификации атаки и максимально автоматизировать и ускорить выработку управляющих воздействии при изменении ситуации в КИТС.

В третьей главе предложен алгоритм минимизации маршрутизаторов в сети, который позволил сократить в три раза время проектирования структуры сети и в два раза число маршрутизаторов. Разработаны математические модели знаний и алгоритма интеллектуальной системы поддержки принятия решений с применением аппарата нечеткой логики. Предложена математическая модель знаний для защиты информации в сети, которая может использоваться при ограниченных сведениях о сети, что характерно для банковских сетей Палестины.

Достоверность и новизна основных выводов и результатов диссертации

Научная новизна результатов исследования заключается в разработке комплекса методик, моделей, программ и структур, позволяющего реализовать интеллектуальную систему поддержки принятия решений в задачах по защите информации в КИТС. Система разработана с применением аппарата нечеткой логики и содержит предложенные автором подсистемы обнаружения и идентификации атак, реагирования на нештатные сетевые ситуации.

Достоверность научных положений, выводов и рекомендаций, сформулированных в диссертации, подтверждается результатами экспериментальных исследований и внедрением.

Практическая ценность

1. Разработанные модели, структуры и алгоритмы могут быть использованы при разработке, эксплуатации и реконструкции современных КИТС в Палестине;
2. Алгоритмы доведены до рабочих программ. Разработана математическая модель действий злоумышленника в системе вычислительных средств защищаемой КИТС, позволяющая оценивать качество функционирования системы защиты информации;
3. Предложенные решения позволили уменьшить время проектирования сетей с маршрутизаторами, число маршрутизаторов, и повысить эффективность защиты.
4. Результаты работы были использованы в корпоративной сети ПФ «Электроприбор» (г. Москва) при повышении уровня информационной безопасности сети; в НПО «РИК» (г. Владимир), что подтверждено соответствующими актами.

Замечания и недостатки

1. Нет пояснений по исходным данным для таблиц и графиков в главе 3 (таблицы 3.4.9, 3.4.10, 3.4.11).
2. Отсутствуют пояснения к рисунку 3.3.11 (в автореферате рисунок 3).
3. Разработанные алгоритмы не иллюстрируются листингами программ (можно было разместить их в приложениях).
4. В диссертации не анализируется достоверность моделей и алгоритмов как таковая, хотя экспериментальная проверка функционирования моделей и алгоритмов осуществлялась с использованием специально разработанной программы, а также проведено внедрение. Авторская формулировка вывода такова (с. 119): «Результаты экспериментальной проверки разработанных моделей и алгоритмов ... показали их работоспособность и практическую значимость».

Заключение

Диссертационная работа представлена на 140 страницах машинописного текста. Содержательная часть, состоящая из введения, трёх глав, заключения и приложений, соответствует названию и указанной специальности.

В целом работа представляет законченное научное исследование, посвящённое разработке интеллектуальной системы поддержки принятия решений по защите КИТС банковского сектора Палестины, включая использование системы обнаружения и идентификации атак, экспертную систему реагирования на нештатные сетевые ситуации, а также создание моделей, алгоритмов и программ поддержки профессиональной деятельности специалистов-руководителей в области сетевого управления.

Автореферат соответствует содержанию диссертации, а опубликованные научные работы отражают основные положения диссертации (9 публикаций, в том числе 3 в изданиях из списка ВАК).

Диссертация соответствует требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, а её автор **Дарахма Ислам** заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Официальный оппонент,
заместитель начальника отдела ЗАО «Автоматика плюс»
кандидат технических наук, доцент В.М. Дерябин

тел. 8 (4922) 42-08-94 e-mail: ltti@avtomatica.ru

Подпись В.М. Дерябина заверяю.
Заместитель директора ЗАО «Автоматика плюс» Д.А. Павлов

5.3.15