На правах рукописи

Дарахма Ислам

Защита банковских компьютерных сетей от несанкционированного доступа в Палестине

Специальность 05.12.13 – Системы, сети и устройства телекоммуникаций

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Владимир 2015

Работа выполнена на кафедре радиотехники и радиосистем ФГБОУ ВПО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ).

Научный руководитель **Галкин Александр Павлович**
доктор технических наук, профессор,
кафедры радиотехники и радиосистем,
«Владимирский государственный
университет имени Александра
Григорьевича и Николая Григорьевича
Столетовых» , г. Владимир

Официальные оппоненты: **Приоров Андрей Леонидович**
доктор технических наук, доцент
кафедры динамики электронных систем,
«Ярославский государственный
университет имени П.Г. Демидова»

Дерябин Вячеслав Михайлович
кандидат технических наук, доцент,
заместитель начальника отдела
измерительной техники ЗАО
«Автоматика плюс», г. Владимир

Ведущая организация: Региональный аттестационный центр
ООО «ИнфоЦентр», г. Владимир

Защита состоится «7 » апреля 2015 г. в 14.00 ч. в ауд. 301-3 на заседании диссертационного совета Д 212.025.04 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, д. 87, корп. 3, ауд. 301.

С диссертацией можно ознакомиться в научной библиотеке ВлГУ и на сайте http://www.vlsu.ru.

Автореферат разослан « 19 » января 2015 г.

Отзывы в двух экземплярах, заверенные печатью, просим направлять по адресу: 600000, г. Владимир, ул. Горького, д. 87, ВлГУ, ФРЭМТ.

Ученый секретарь диссертационного совета

доктор технических наук, профессор А. Г. Самойлов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. 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 (к сожалению, в Палестине, часто и с недостаточными скоростями и памятью, с использованием телефонных линий), большой объем поступающей информации и различные несанкционированные информационные п проникновения создают трудности в обеспечении нормальной работы банковских сетей.

Указанные проблемы делают практически невозможным применение только традиционных математических методов, в том числе методов математической статистики и теории вероятностей, а также классических методов оптимизации сетевых структур для решения прикладных задач защиты информации в КИТС.

Актуальность работы связана с необходимостью:

- Обеспечить процесс принятия решения о структуре сети и принципов поиска информационных проникновений при отсутствии классического математического аппарата, что приводит к тому, что при оценке и выборе альтернатив возможно, (а зачастую просто необходимо) использовать и обрабатывать качественную экспертную информацию.

- Использовать перспективное направление разработки методики принятия решений при экспертной оценке исходной информации и внедрение интеллектуальной системы поддержки принятия решения (ИСППР) (лингвистический подход на базе теории нечетких множеств) для управления и диагностики состояния современной КИТС.

- Разработать комплекс средств защиты информации с идентификацией пользователей при запросах на доступ в КИТС, что очень актуально и должно реализовываться современными системами защиты информации (СЗИ) от НСД. Исследование и применение нами нечеткой логики к задаче обнаружения и идентификации при запросах доступа к ресурсам, представляется одним из способов, позволяющим улучшить защиту.

Объект исследования. Объектом исследования являются корпоративные (банковские) информационно-телекоммуникационные сети, защита которых осуществляется в условиях неполной и нечеткой информации об угрозах и о проникновениях.

Предмет исследования. Предметом исследования являются методики, алгоритмы и процедуры обеспечения управления информационной безопасностью, математическое и программное обеспечение системы поддержки принятия решений для управления диагностикой(поиском информационных проникновений) корпоративных информационно-телекоммуникационных сетей в условиях отсутствия полной, четкой и достоверной информации о состоянии элементов сети и сетевых процессов.

Настоящая диссертационная работа посвящена разработке методик оценок, принципов функционирования и технологии создания комплексных интеллектуальных систем поддержки принятия решения о структуре сети и принципов поиска информационных проникновений, основанных на экспертных знаниях, предназначенных для мониторинга, анализа и идентификации пользователей при запросах на доступ в корпоративных информационно-телекоммуникационных сетях применительно к особенностям Палестины.

Научная проблема. Суть научной проблемы заключается в том, что, с одной стороны, необходимо полностью обеспечить требования безопасного функционирования КИТС в условиях атак злоумышленников на информационные ресурсы и процессы, с другой стороны, наблюдается нехватка методик оценок и алгоритмов минимизации структур, позволяющих это сделать с достаточной полнотой и достоверностью.

Целью диссертационной работы является:

- разработка интеллектуальной СППР на базе комплексного подхода к проблеме управления информационной безопасностью;

-выбор: системы обнаружения атак, идентификацию атаки, интеллектуальных (экспертных) систем реагирования на нештатные сетевые ситуации;

-создание методик, моделей, алгоритмов и программ поддержки профессиональной деятельности специалистов-руководителей в области сетевого проектирования и управления.

Для достижения цели необходимо решить следующие задачи:

1. Проанализировать современное состояние проблемы управления информационной безопасностью и защиты информации в КИТС в банках, в первую очередь в условиях атак злоумышленников на информационные ресурсы и процессы, выявить общие пути ее решения (применительно к особенностям Палестины).

2. Разработать алгоритмическую и методологическую основу построения системы управления информационной безопасностью и защиты информации.

3. Предложить новый подход к нечеткому структурно-логическому обобщению знаний на основе нечеткой интерпретации данных и знаний для конкретных сетей.

4. Разработать комплекс методик, программ и структур, позволяющий реализовать интеллектуальной системе поддержки принятия решений в задачах по защите информации в КИТС, использующий нечеткую логику.

Научная новизна работы заключается в том, что:

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 интеллектуальной системы поддержки принятия решений в задачах по защите информации в КИТС, использующий нечеткую логику.

Методы исследования основаны на элементах нечеткой логики, дискретной математики, теории вероятностей, теории надежности, теории системного анализа и методах лабораторного эксперимента.

Достоверность научных положений, выводов и практических результатов и рекомендаций подтверждена 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.

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;

- наши разработки позволили уменьшить время проектирования сетей с маршрутизаторами в 3 раза, число маршрутизаторов в 2 раза, повысить эффективность защиты более чем на 70%.

Реализация результатов работы. Результаты, полученные в ходе работы над диссертацией, были использованы в корпоративной сети завода «Электроприбор» (г. Москва) при повышении уровня информационной безопасности сети; в НПО «РИК» (г. Владимир). поскольку по своей сетевой структуре они аналогичны палестинским банкам, и работа будет внедрена в Палестине после защите.

Апробация работы. Основные результаты, полученные в ходе работы над диссертацией, были доложены на пяти международных НТК.

Публикации. По теме диссертации опубликовано 9 научных статей и тезисов докладов, из них 3 статьи опубликованы в журналах «Известия института инженерной физики» и «Проектирование и технология электронных средств» из перечня, рекомендованных ВАК РФ для публикации результатов диссертационных работ.

Диссертация состоит из введения, 3 глав, заключения, списка использованной литературы из 110 наименований, списка сокращений (стр.140, рис.36, табл. 33) и приложений.

На защиту выносится:

1. Интеллектуальная СППР для управления информационной безопасностью в сети;

2. Система обнаружения атак.

3. Система идентификация атаки.

4. Система реагирования на нештатные сетевые ситуации.

5. Методики, алгоритмы и программы поддержки профессиональной деятельности специалистов-руководителей в области сетевого проектирования и управления.

Краткое содержание работы

Во введении показаны проблемы телекоммуникационных сетей Палестины, актуальность и 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.

Несанкционированный доступ к информации (НСД) – это доступ к информации, нарушающий правила доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств телекоммуникаций, вычислительной техники или автоматизированных систем.

Рассмотрены особенности банковских сетей Палестины и обеспечение их информационной защиты.

Во второй главе предлагается структурная схема комплексной интеллектуальной СППР, которая содержит множество функциональных компонент, позволяющих диагностировать состояния КИТС, идентификации атаки и максимально автоматизировать и ускорить выработку управляющих воздействии при изменении ситуации в КИТС.

Выявление вторжения осуществляется на основании анализа результатов мониторинга состояния КИТС и внешних воздействий на нее. Состояние КИТС анализируются не непосредственно, а с использованием штатных средств типа системных логов и протоколов аудита.

На первом этапе выполняется процедура сбора первичных данных о работе КИТС. Для реализации выбранного метода определения и идентификации сетевых аномалий (СА) разработаны модели сигнатурного и статистического анализаторов сетевого трафика, а для определения источников СА и выбора вариантов по их устранению – нечеткая интеллектуальная система. Структура универсального сигнатурного анализатора потока пакетов сетевого трафика представлена на рис.1. Механизм функционирования сигнатурного анализатора включает два этапа: Фильтрация и сборка фрагментов пакетов, распознавание СА по сигнатурам.

Работа анализатора описывается следующей моделью. Обозначим сетевой трафик, поступающий из сенсоров, Сетевой трафик представляется как совокупность сообщений S обозначаемых как $S_{k,1}^{n_{U_{k,1}}}$, где $n_{U_{k,1}}$ номер сообщения от $U_к$

- последнего по порядку источника сообщений к U_1 - первому по порядку источнику сообщений, где k - количество узлов в КИТС.

Базу сигнатур представим в виде множества B, объединяющего кластеры типов сигнатур $B_j = \{b_{jk}\}_1^K$, $j = \overline{1,m}$:

$$B = B_1 \cup B_2 \cup ... \cup B_m = \bigcup_{j=1}^{m} B_j$$

где m – количество кластеров сигнатур; B_j – j-й кластер, являющийся множеством однотипных сигнатур; K – общее количество сигнатур в j-м кластере. На вход модуля реагирования поступает сигнал только в том случае, если $S \subseteq B$.

M-число информационных пакетов;

m- число каналов.

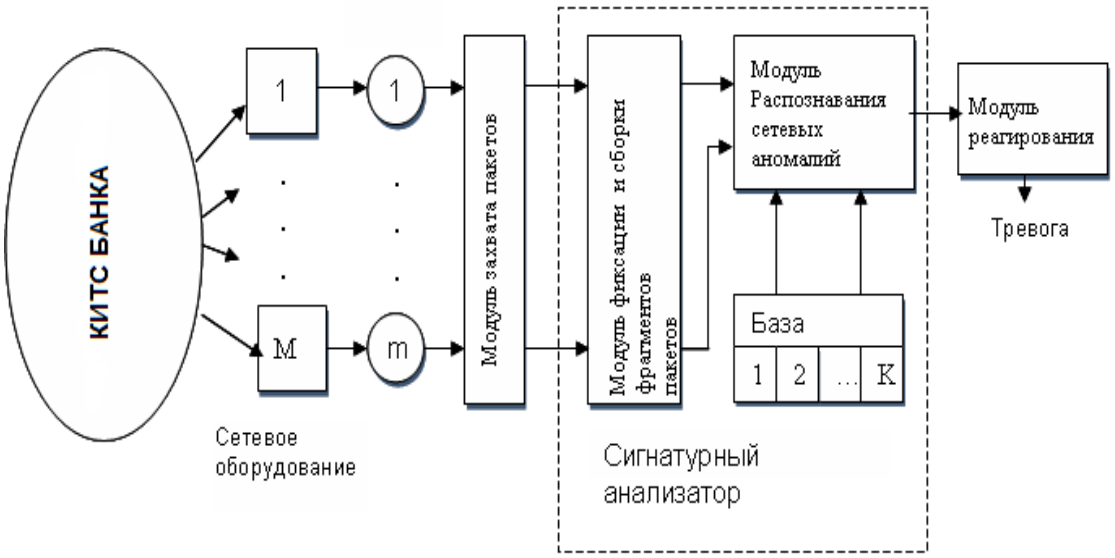

Рис.1. – Структура универсального сигнатурного анализатора

Рассматривается модель вычисления рисков.

Предположим, имеется M пар (актив, угроза). Для каждой такой пары риск вычисляется по обычной формуле

$$R_k = P_i * I_j,$$

где k — номер пары; P_i - вероятность реализации угрозы по отношению к "парному" активу; I_j - воздействие реализации этой угрозы на актив; R_k - величина риска.

Пусть, далее, риски считаются допустимыми, если для всех k $R_k <= R_a$, где R_a - порог допустимости.

Пусть *N* — число положительных r_k, то есть число пар (актив - полезная информация, угроза-подозрительная информация), риски которых нуждаются в нейтрализации. Отбросим нулевые избыточные риски и перенумеруем оставшиеся. Можно вычислить среднее значение избыточного риска r_{Mean}, воспользовавшись формулой

$$r_{Mean} = \frac{\sum_{k=1}^{N} r_k}{N}$$

Значение r_{Mean} можно рассматривать не только как средний избыточный риск, но и как оценку защищенности КИТС в целом. Эту оценку можно определить по формуле

$$r_{MeanNrorm} = \frac{r_{Mean}}{R_{\max} - R_a}$$

где $R_{\max}$ - максимальный из возможных рисков R_k, то есть произведение максимального из возможных значений P_i и I_j в выбранной шкале измерений. Значения $r_{MeanNrorm}$, близкие к 0, характеризуют уровень информационной безопасности КИТС как весьма высокий. Близкие к 1 значения, напротив, характерны для слабо защищенных информационных систем. При желании весь диапазон можно разбить на интервалы, выделив тем самым нужное число уровней безопасности.

В третьей главе нами предложен алгоритм минимизации маршрутизаторов в сети, который позволил сократить в 3 раза время проектирования структуры сети и в 2 раза число маршрутизаторов, а также разработаны математические модели знаний на основе нечеткой логики и алгоритма интеллектуальной системы поддержки принятия решений о структуре сети и принципов поиска информационных проникновений в задачах по защите информации в КС.

Модель для защиты информации в сети, которая может использоваться при ограниченных сведениях о ней. Это очень характерно для банковских сетей Палестины.

Обозначения:

$O = \{o_i\}$ - база знаний,

$A = \bigcup_{i=1}^{N} A_i$ - множество всех атрибутов в базе знаний;

$\{a_{11}, a_{12}, \ldots\ldots, a_{1m}\}$
$\{a_{21}, a_{21}, \ldots\ldots, a_{2j}\}$;
……..……..
$\{a_{k1}, a_{i2} \ldots\ldots, a_{km}\}$

Где $\{a_{ij}\}$- множество a_j-го атрибута по множеству объекта $\boldsymbol{o_i}$-м.

Где, $i = \overline{1, N}$ - число объектов в базе знаний;

$j = \overline{1, m}$ -множество атрибутов параметрических;

Активный атрибут по $\boldsymbol{o_i}$-му объекту - это атрибут $a_j \in A_i \subseteq A$, т.е. атрибут $\boldsymbol{a_j}$ принадлежит к подмножеству атрибутов $\boldsymbol{o_i}$-го объекта.

Матрицу активности может принимать два значения: 0 - если атрибут a_j не принадлежит множеству атрибутов $\boldsymbol{o_i}$-го, и 1 - если атрибут a_j принадлежит множеству атрибутов $\boldsymbol{o_i}$-го.

Обозначим $\boldsymbol{R}$ матрицу активности атрибутов в базе знаний **O:**

$$\boldsymbol{R} = \|\boldsymbol{r}_{ij}\|,$$

где

$$r_{ij} = \begin{cases} 1, & если \quad a_j \in A_i \\ 0, & если \quad a_j \notin A_i \end{cases}$$

Обозначим ***W*** матрицу значений атрибутов по объектам базы знаний:

$$W = (\omega_{ij}),$$

Где $\omega_{ij} \in W_i$ - значения a_j-го атрибута по множеству значений o_i-го объекта.

Экспериментальное исследование предложенных моделей и алгоритмов осуществлялось с использованием специально разработанной программы. Для демонстрации возможностей предложенной методики организации базы знаний рассмотрено на расчете для сети завода «Электроприбор» (г. Москва).

Дано множество объектов О (пользователей корпоративных информационно-телекоммуникационных сетей), атрибутов ***A***, множество их значении ***W*** и неизвестный объект ***X*** (как новый пользователь). Необходимо выполнить: 1) Кластеризацию и структуризацию множества **О.**

2) Провести процесс *идентификации объекта* ***X*** на основе множества объектов ***O***. $O = \{O_1, O_2, O_3, O_4, O_5, O_6\}$; (множество объектов О пользователей КИТС)

$A = \bigcup_{i=1}^{N} A_i = \{a_j\} = \{a_1, a_2, a_3, a_4, a_5, a_6\}$; (множество a_j-го атрибута по множеству объекта О) $A_i = (a_{ij}), \quad a_{ij} \in A, \quad N = |O| = 6, \quad j = \overline{1,M}, \quad M = |A| = 6$.

$A_1 = \{a_2, a_3, a_5, a_6\}$, $W_1 = \{0{,}61;0{,}081;0{,}75;0{,}3\}$;

$A_2 = \{a_1, a_2, a_5\}$, $W_2 = \{0{,}005;0{,}51;0{,}83\}$;

$A_3 = \{a_1, a_2, a_3, a_4, a_6\}$, $W_3 = \{0{,}75;0{,}56;0{,}77;0{,}59;0{,}64\}$;

$A_4 = \{a_1, a_2, a_4, a_6\}$, $W_4 = \{0{,}64;0{,}66;0{,}34;0{,}25\}$;

$A_5 = \{a_1, a_2, a_3, a_5, a_6\}$, $W_5 = \{0{,}53;0{,}225;0{,}2;0{,}4;0{,}55\}$;

$A_6 = \{a_2, a_3, a_5\}$, $W_6 = \{0{,}83;0{,}08;0{,}6\}$.

$$X : A_x = \{a_1, a_4, a_6\}; \qquad W_x = \{\omega_{x1}, \omega_{x4}, \omega_{x6}\} = \{0{,}76; 0{,}42; 0{,}64\}.$$

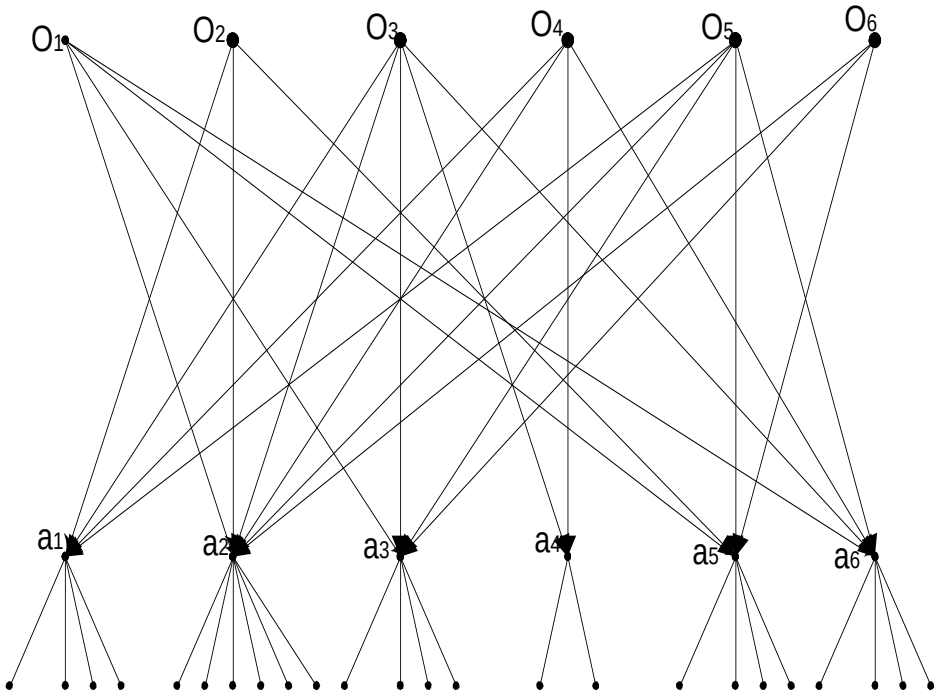

Рис. 2. Объекты базы КИТС

С- угрозы для сети и проникновения в сеть. Получаем результат монокритериального выбора альтернатив:

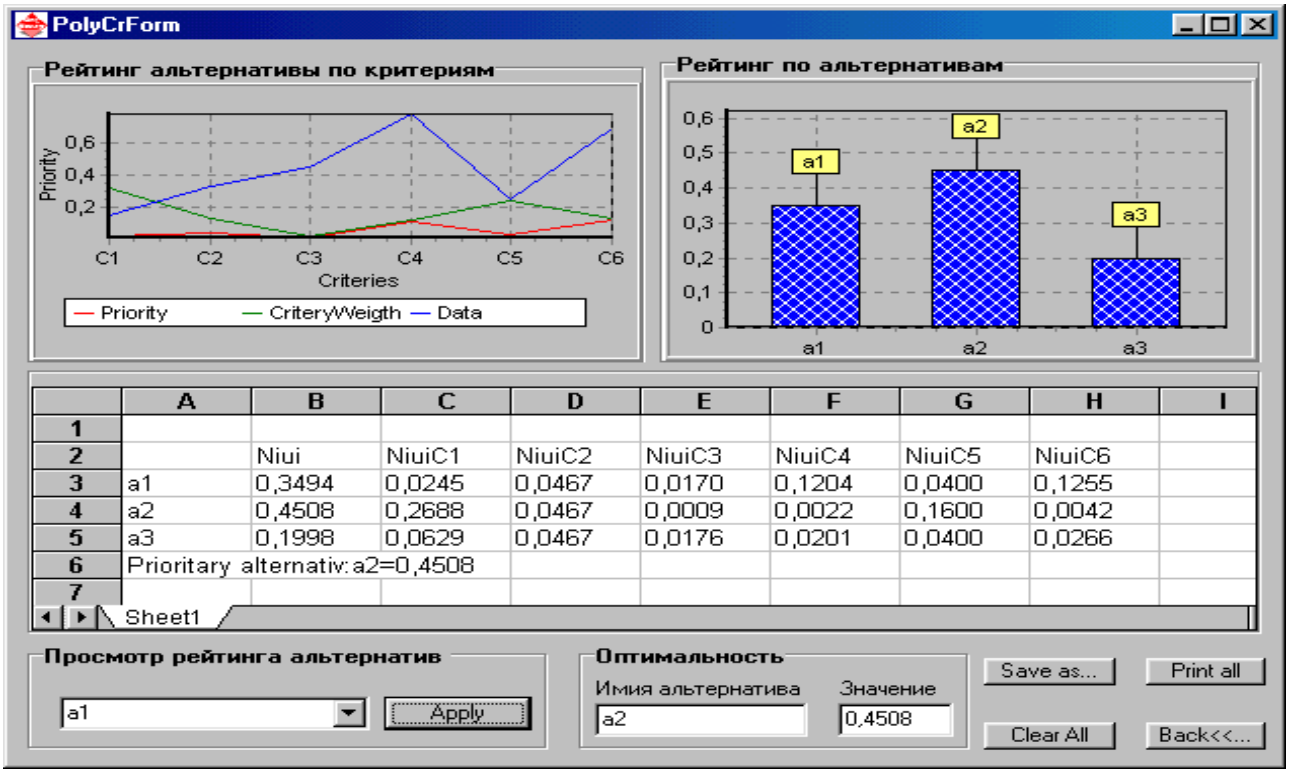

Рис. 3.

Из анализа рис.3 можно сделать выводы: какие можно получить приоритеты, каковы рейтинги при различных альтернативах, оптимальный рейтинг по альтернативам.

Заключение

В диссертационной работе поставлены и решены следующие основные вопросы и проблемы:

1. В условиях Палестины жизненно необходима защита корпоративных и банковских сетей. Поскольку существует большая неопределенность различных угроз, проникновений и возможной защиты от них, то целесообразно применение аппарата нечеткой логики.

2. Разработаны методики, алгоритмы и структуры для корпоративных и банковских сетей применительно к условиям Палестины.

3. Разработана структура для диагностики состояния КИТС, реализующая проведение сигнатурного и статистического анализа сетевого трафика и реагирования на нештатные сетевые ситуации.
4. Результаты экспериментальной проверки разработанных моделей и алгоритмов оптимизации состава средств защиты и управления безопасностью на основе анализа рисков показали их работоспособность и значимость.
5. На этой основе выработаны рекомендации и предложения по созданию новых и усовершенствованию существующих систем защиты информации в КИТС завода «Электроприбор» (г. Москва) (чья телекоммуникационная сеть аналогична по структуре палестинским банковским сетям). При этом обеспечивается выигрыш в эффективности защиты по сравнению с существующими на 70%.

6. Разработана методика и сделана минимизация маршрутизаторов в конкретной сети с обеспечением защиты, что позволило уменьшить время

проектирования в 3 раза, а число маршрутизаторов в 2 раза.

7. Разработаны и внедрены методики и программные модули, которые позволили провести тестирование алгоритмов принятия решений в задачах управления в условиях неопределенности на основе аппарата нечеткой логики. Результаты тестирования этих модулей на реальных данных формирования и конкретных предприятий повысили их эффективность (на 70%) по сравнению с традиционными методами принятия управленческих решений и позволили повысить их конкурентоспособность.

СПИСОК РАБОТ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Дарахма, Ислам Минимизация маршрутизаторов при обеспечении информационной защиты в сетях / Галкин А.П., Али Альджарадат М,М,. Бадван А. // Известия института инженерной физики. - 2013. - №1. - С. 2-4.

2. Дарахма, Ислам Синтез пользовательской структуры для информационной защиты сети с маршрутизаторами с использованием САПР / Галкин А.П., Альджарадат М.М., Бадван А., Яремченко С.В. Амро М.М. // Известия института инженерной физики. - 2014. - №1. - С. 11-14.

3. Дарахма, Ислам Обоснование аппаратурных затрат на реализацию итеративного кода для обнаружения и коррекции ошибок при информационной защите / Галкин А.П., Альджарадат М.М., Амро М.М. // Проектирование и технология электронных средств №4, - 2013. - С. 20-23.

4. Дарахма, Ислам. Беспроводные сети и технико-экономическое обоснование их для здравоохранения / Галкин А.П., Альджарадат М.М. // Труды X Международной научной конференции «Физика и радиоэлектроника в медицине и экологии» / Владимир-Суздаль, - 2012 г. - С. 176-177.

5. Дарахма, Ислам Проблемы информационной безопасности и инновационные пути их решение / Галкин А.П., Аль-Джабери Р., Альджарадат М.М. // Инновационное развитие экономики – основа устойчивого развития территориального комплекса /Материалы межрегиональной научн. конф.-Институт экономики АН РФ, Владимир-Москва, - 2012, - С.172-176

6. Дарахма, Ислам Ветроэнергетика в России и во Владимире / Галкин А.П., Альджарадат М.М., Х.М. Обади // Урбанистика городов с историческим ядром». Матер. межд. конф. Владимир, -2012. - С. 205-208.

7. Дарахма , Ислам Повышение отказоустойчивости транспортного уровня вычислительных сетей путем реорганизации сквозной «точка-точка» множественной адресации / Галкин А.П., Альджарадат М.М., Амро М.М.// Перспективные технологии в средствах передачи информации/Материалы 10-й Межд. научно-технической конф. Владимир, - 2013 г., - Т.2, С.49-52.

8. Дарахма, Ислам Конкурентность предприятия и его информационная защищенность / ГалкинА.П., Альджарадат М.М., Амро М.М., Бадван А.// Второй Российский экономический конгресс/Материалы международной научн. конф/Институт экономики АН РФ, Суздаль-Владимир, - 2013, - С.112-115.

9. Дарахма, Ислам Пользовательская структура для информационной защиты медицинской сети с маршрутизаторами / Галкин А.П., Амро М.М., Альджарадат М.М. // Труды X Международной научной конференции «Физика и радиоэлектроника в медицине и экологии»/ Владимир-Суздаль, - 2014 г. - Кн. 2, - С.147-150.

Подписано в печать 12.01.2015г.
Формат 60×84/16. Усл. печ. л. 1,09. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.