МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

**Дарахма Ислам**

# Защита банковских компьютерных сетей от несанкционированного доступа в Палестине

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель - профессор,
д. т. н. Галкин А.П.

г. Владимир-2015 г.

**Содержание**

Стр.

# ВВЕДЕНИЕ

Корпоративная информационно-телекоммуникационная сеть (КИТС) есть результат эволюции двух научно-технических отраслей современной цивилизации - компьютерных и телекоммуникационных технологий. Они могут использоваться совместно и требуют защиты.

КИТС - сложная система, в ней множество различных ресурсов и одновременно протекающих системных и прикладных информационных и телекоммуникационных процессов. Поскольку создание единого информационного пространства и подключение корпоративных сетей к глобальной сети Интернет используется все чаще, то следует ожидать в будущем атак(информационных, точнее, разрушающих информацию) на такие системы с целью уменьшения их эффективности.

В нашем случае, для Палестины характерны комплексы компьютерных и телекоммуникационных сетей (телефонных, радио, телевизионных сетей), проводных и беспроводных[107, 108].

Чтобы достигнуть хорошей защиты КИТС, необходимо защищать информацию, в соответствии с ее ценностью в корпорации (в банке)[109, 110] и с определенным ранжированием. А это приводит к большим затратам на компенсацию действия угроз безопасности информации КИТС. Следовательно, крайне важно уменьшать эти затраты и улучшать эффективность защиты.

Телекоммуникации обеспечивают движение прогресса вперед всей мировой цивилизации, что исключительно важно для Палестины, где многое из названных технологических процессов находится в стадии становления [107-110].

Внедрение методов, методик, структур, алгоритмов для обеспечения эффективного функционирования системы защиты в конкретных КИТС требует разработки строгих мер защиты для предотвращения случайных и умышленных нарушений их функционирования. Для уменьшения ущерба от всяких вредных воздействий важно четко и грамотно выбирать меры и

средства обеспечения защиты информации (ЗИ) от умышленного разрушения, кражи, порчи и несанкционированного доступа (НСД) в корпорациях, банках и в социальных сетях.

Проблема обеспечения информационной безопасности является самой главной в КИТС и в корпоративных сетях (КС) простого назначения. При этом требуется управление основанное на наблюдении за сетью и сборе информации во всех структурах и процессах сети.

В КИТС должно обеспечиваться система управления сетью, которая выполняет полный и непрерывный контроль либо по определенной программе за всеми элементами сети, своевременное обнаружение угроз, проникновений, ошибок, неисправностей, сбоев и отказов оборудования, программного обеспечения, управление конфигурациями сетевых узлов, резервное копирование и восстановление всех элементов сети, управление сетевым трафиком и политикой безопасности.

Обычные, хорошо известные, математические модели при неопределенных условиях не дают хорошего результата. Поэтому необходима разработка новых, ориентированных на специфику процессов защиты информации методов и средств моделирования, в частности подход с нечеткой логикой.

Таким образом, сложное оборудование КИТС (к сожалению, в Палестине, часто и с недостаточными скоростями и памятью[110]), большой объем поступающей информации, трудность решения плохо формализуемых и слабо структурированных задач при отсутствии полной и достоверной информации о состоянии элементов сети, короткое время на анализ проблемных ситуаций и принятие решения приводят к несоответствию возможностей человека требованиям эффективно управлять сетью.

Это делает затруднительным применение хорошо разработанных математических методов, в том числе, также классических методов оптимизации для решения требуемых нам задач защита информации в КИТС.

Актуальность работы связана с необходимостью:

- Перспективным направлением разработки методики принятия решений при экспертной исходной информации и внедрение интеллектуальной системы поддержки принятия решения ИСППР (лингвистический подход на базе теории нечетких множеств и лингвистической переменной). Это объясняется сложностью процесса принятия решений, отсутствием математического аппарата, что приводит к тому, что при оценке и выборе альтернатив возможно, (а зачастую просто необходимо) использовать и обрабатывать качественную экспертную информацию.

Поэтому оптимальные нечеткие управления и диагностика состояния современной КИТС в Палестине следует считать актуальной научно-технической задачей.

- Комплексы СЗИ с идентификацией пользователей при запросах на доступ в КИТС, актуально и должно реализовываться современными СЗИ от НСД.

Управление доступом включает идентификацию пользователей, персонала и ресурсов системы, становится все более актуальной с учетом проникновений в КИТС. Применяемые методы построения систем обладают рядом недостатков.

Исследование и применения нами нечеткой логики к задаче обнаружения олицетворения при запросах доступа к ресурсам, представляется одним из способов, позволяющих избавиться от этих недостатков.

Дополнительно нами предложены некоторые структуры сетей, с учетом особенностей Палестины, с их частичной оптимизацией, а высокий уровень автоматизации и интеллектуализации системы позволит снизить нагрузку на специалистов по управлению КИТС (сетевых администраторов), повысит эффективность их действий, увеличит надежность функционирования сети и снизит экономические риски для предприятий и банков.

**Объект исследования.** Объектом исследования являются корпоративные (банковские) информационно-телекоммуникационные сети Палестины,

защита которых будет проводиться в условиях неполной и нечеткой информации о сетевых процессах.

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

Эта работа посвящена разработке методик оценок, алгоритмов, минимизации структур, принципов функционирования и технологии создания комплексных ИСППР о структуре сети и принципов поиска информационных проникновений, основанных на экспертных знаниях, в корпоративных информационно-телекоммуникационных сетях применительно к особенностям Палестины.

**Научная проблема.** Суть научной проблемы заключается в том, что, с одной стороны, необходимо обеспечить требования, установленные заказчиком, 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 приемлемыми результатами, устраивающими заказчиков и с заданной достоверностью.

Исходя из вышеизложенного, настоящая диссертационная работа посвящена разработке принципов функционирования и технологии создания комплексных интеллектуальных систем поддержки принятия решения, основанных на экспертных знаниях, предназначенных для проверки, анализа и диагностики состояния элементов КИТС, с заданными достоверностями и при ограничениях на затраты.

**Целью диссертационной работы** является разработка интеллектуальной СППР на базе комплексного подхода к проблеме

управления информационной безопасностью и защиты информации и КИТС от преднамеренного несанкционированного вмешательства в процесс функционирования КИТС или несанкционированного доступа к циркулирующей в ней информации включающего использование **системы обнаружения атак** для детектирования и идентификации атаки, интеллектуальных (экспертных) систем реагирования на нештатные сетевые ситуации, а также создание моделей, алгоритмов и программ поддержки профессиональной деятельности специалистов-руководителей в области сетевого 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 и методику оценки ее эффективности.

3. Предложить новый подход к нечеткому структурно-логическому обобщению знаний на основе нечеткой интерпретации данных и знаний, которые хорошо себя показали при решении таких задач.

4. Разработать методику нечеткой идентификации, к задаче обнаружения олицетворения при запросах доступа к ресурсам КИТС.

5. Разработать комплекс программ и структур, позволяющий реализовать интеллектуальной системе поддержки принятия решений в задачах по защите информации в КИТС, использующий нечеткие модели.

**Научная новизна работы** заключается в том, что:

1. Предложена методика управления информационной безопасностью КИТС, использующая интеллектуальные нечеткие модели, с элементами нечеткой логики.
2. Предложен очень эффективный подход к нечеткому структурно-логическому обобщению знаний на основе нечеткой геометрической интерпретации данных и знаний.
3. Разработаны методика структурной минимизации при использовании роутеров и методика нечеткой идентификации, к задаче обнаружения олицетворения при запросах доступа к ресурсам КИТС.
4. Разработан комплекс программ и структур, позволяющий реализовать ИСППР в задачах по защите информации в КИТС, использующий нечеткие модели.

**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 модернизации, уже используемых современных КИТС в Палестинских условиях;
- 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.

**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. А в последствии работа будет внедрена в Палестине, после защиты.

**Апробация работы.** Основные результаты, полученные в ходе работы над диссертацией, были доложены на пяти международных НТК и на семинарах кафедры РТ и РС.

**Публикации.** По теме диссертации опубликовано 10 научных статей и тезисов докладов, из них 3 статьи опубликованы в журналах «Известия института инженерной физики» и «Проектирование и технология электронных средств» из перечня, рекомендованного ВАК РФ для публикации результатов диссертационных работ, а также в зарубежном периодическом издании.

Диссертация состоит из введения, 3 глав, заключения, списка использованной литературы из 110 наименований, списка сокращений (стр. 140, рис.36, табл. 53) и приложений 18 стр..

# 1. Несанкционированный доступ к информации в банковских сетях Палестины

## 1.1. Анализ технических каналов банковских корпоративных сетей по несанкционированному доступу и защите от него

Информационные процессы обеспечивают главную роль в безопасности всего общества, поэтому защита информации является одним из важных направлений в корпоративных сетях связи и в улучшении всеобщей гармонии человечества.

Это особенно важно для Палестины, которая находится в очень близком соседстве с неустойчивыми странами и с неустойчивостью собственного режима. Предприятие, которое мало уделяет внимания защите от несанкционированного доступа, всегда проигрывает конкурентам, а для государства это и безопасность и доверие всех граждан своей страны и окружающих!

**Основные объекты защиты информации** [19-24, 85, 86]:

Сформируем для них табл. 1.1.1:

Таблица 1.1.1. Объекты информатизации

| Объекты | Вид тайны | О ком сведения |
|---|---|---|
| информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне | корпоративную и конфиденциальную информацию | о клиентах банков, в том числе и глубоко личные |
| средства и системы, которые часто называют техническими средствами приема, обработки, хранения и передачи информации (ТСПИ) | корпоративную и конфиденциальную информацию о структуре сетей и об их наполняемости | О структуре сетей банков |

| | | |
|---|---|---|
| ТСПИ, размещенные в местах, в которых есть конфиденциальная информация - вспомогательные технические средства и системы (ВТСС) | информацию о структуре сетей и об их наполняемости | О структуре сетей банков и об их телекоммуникациях |

Для приема и измерения параметров сигналов, для их анализа и оптимизации используют технические средства разведки (ТСР) [17, 18, 25, 26, 85, 86].

По взаимодействию и от природы информационных сигналов, а также среды их распространения и способов перехвата ТСР технические каналы утечки классифицируются с разных позиций. Покажем это в табл.1.1.2:

Таблица 1.1.2. Взаимодействие и природа информационных сигналов, требующих защиты

| Вид | Природа действия | Принципы защиты |
|---|---|---|
| электромагнитные | Активные, пассивные | ослабление информационных сигналов ТСПИ до фона, близкого к естественным шумам; создание электромагнитных помех для уменьшения отношения сигнал/шум информационного сигнала ТСПИ |
| электрические | Активные | ослабление информационных сигналов ТСПИ в цепи электропитания |
| параметрические | пассивные | ослабление информационных сигналов ТСПИ в цепи электропитания |

| | | |
|---|---|---|
| воздушные (прямые акустические), вибрационные (виброакустические) | Активные | ослабление информационных сигналов ТСПИ до фона, близкого к естественным шумам |
| оптико-электронные и параметрические - для речевой информации | Активные, пассивные | ослабление информационных сигналов ТСПИ до фона, близкого к естественным шумам |
| проводные | Активные | создание помех в проводниках и соединительных линиях ВТСС с целью уменьшения отношения сигнал/шум информационного сигнала ТСПИ |

Хорошо видно, что потребуется приложить очень основательные усилия по защите информации, причем для нас, с учетом особенностей Палестины (широкое использование телефонных модемов, маршрутизаторов, малые скорости и объемы памяти, неопределенность обстановки) и того больше. Этому и посвящаем эту диссертационную работу

## 1.2. Ограничения и особенности на палестинских секторах информационных и коммуникационных технологий.

За последние десять лет, Палестинской национальной администрации были проведены интенсивные усилия, чтобы удалить различные запреты и ограничения на палестинских информационных и коммуникационных технологий (ИКТ) [107-110]. Правовые основы для палестинских усилий в этом включают в себя: международное право, с акцентом на права Палестины в качестве наблюдателя в Международный союз электросвязи; статьей 36 Приложения III Временного соглашения описанием механизмов координации, а также приложение IV Временного соглашения (Париж Protocol), который определяет экономические отношения.

Основные участники этой координация - Международный союз электросвязи (МСЭ), Управления квартета (OQR), Всемирного банка и Генерального консульства США в Иерусалиме.

1. Закрепление частот в Палестине, которое позволило бы:
* Развертывание расширенных мобильных голосовых приложений;
* Развертывание новых технологий, в том числе третьего поколения (3G), систем и услуг четвертого поколения (4G), систем и услуг и долгосрочной эволюции (LTE), а также
* Интеграция и развитие магистральной телекоммуникационной и транспортной.

2. Строительство ИКТ - инфраструктуры на палестинских территориях.

3. Импорт оборудования для разработки и мониторинга телекоммуникационных операций.

4. Координация возможных помех в Палестине.

5. Борьба с незаконными операциями операторов мобильной связи и интернет провайдеров.

Министерство телекоммуникаций и информационных технологий приняло решение опубликовать и сделать доступными большинству своих документов, имеющих отношение к ограничениям на сектор ИКТ. Кроме того, это позволило:

1. Увеличить вклад сектора ИКТ в ВВП палестинских более чем на 2%;
2. Обеспечить сотни рабочих мест для квалифицированного и неквалифицированного труда;
3. Уменьшить разрыв в цифровых технологиях между Палестиной и остальным миром, особенно с соседними странами. Это создаст необходимые условия для устойчивого экономического развития;
4. Предоставление новых услуг с добавленной стоимостью, которые соответствуют возникающих потребностей потребителей с более высоким качеством и более низким ценам;
5. Увеличить государственные доходы от налогов, лицензионных сборов и

спектр аренды;

6. Очистить палестинский телекоммуникационный рынок от незаконных услуг мобильной связи, которые контролируют более 20% палестинского рынка ИКТ и которая истощает доходы Палестинской автономии с более чем 150 миллионов долларов США в год[107-110];

7. Включить новые электронные решения для образования, здравоохранения и предприятий среди прочего, посредством применения 3G и 4G;

8. Увеличить скорость проникновения Интернета в качестве основной инфраструктуры для устойчивого социального, экономического и образовательного развития;

9. Ускорить автоматизацию государственных процедур путем публикации электронных приложений правительства, которое приведет к снижению затрат и времени;

10. Содействие развитию связей в Палестине.

## 1.3. Особенности несанкционированного доступа и защита от него.

Несанкционированный доступ к информации (НСД) – это доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Все это относится и к КИТС Палестины.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств телекоммуникаций, вычислительной техники или автоматизированных систем. Защита от несанкционированного доступа (Защита от НСД) – это предотвращение или существенное затруднение несанкционированного доступа или сохранение целостности информационных потоков[25, 26].

Защита от НСД информации в процессе ее обработки приобретает большое значение в задачах обеспечения информационной безопасности, в связи с пониманием необходимости такой защиты руководителями предприятий и организаций, расширением пространства угроз

информационной безопасности и ужесточившимися законодательными требованиями, как, например в России.

Можно отметить актуальность, важность и трудности вопросов защиты персональных данных в связи с принятием Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (в Палестине пока нет аналогичного законодательства[110]), вместе с тем, не менее важными остаются вопросы защиты коммерческой и иных видов тайн, в том числе и банковской.

Некоторые технологии и методы, направленные на защиту информации, уже встроены в современные операционные системы, но таких мер зачастую оказывается недостаточно. По мнению экспертов в области ИБ в наиболее распространенном на сегодняшний момент семействе ОС Windows постоянно обнаруживаются уязвимости, позволяющие получить доступ к защищаемой информации в обход правил разграничения доступа и политик безопасности.

Поэтому, а также насущными и справедливыми требованиями законодательства, создаются дополнительные программные или программно-аппаратные СЗИ от НСД (табл.1.3.1,2).

Таблица 1.3.1. СЗИ от НСД может содержать подсистемы[26,86, 99]:

| Подсистемы | Ответственность |
|---|---|
| Подсистема управления доступом | администрация |
| Подсистема регистрации и учета | администрация |
| Криптографическая подсистема | Проект, заказчик |
| Подсистема обеспечения целостности | заказчик |
| Подсистема антивирусной защиты | администрация |
| Подсистема обнаружения вторжений (проникновений) | Проект |

Для реализации защиты информации от несанкционированного доступа используются следующие решения (табл.1.3.2):

Таблица 1.3.2. Реализации защиты информации от несанкционированного доступа

| **Подсистемы/ функции** | Варианты решения |
|---|---|
| **Управление доступом к серверам и рабочим станциям** | «Блокхост-сеть» (ГИС)<br>Сертифицированные защищенные ОС<br>Aladdin eToken<br>Secret Net<br>ruToken<br>Cisco Security Agent |
| **Управление доступом в сеть** | Коммутаторы серии Cisco Catalyst (с поддержкой NAC)<br>Cisco Trust Agent<br>Cisco ACS<br>Microsoft NAP<br>«Блокхост-сеть» |
| **Регистрация и учет** | Сертифицированные ОС (механизмы аудита)<br>Secret Net<br>Cisco Security Agent |
| **Обеспечение целостности** | «Блокхост-сеть» (ГИС)<br>Сертифицированные ОС<br>Cisco Security Agent<br>Касперский Total<br>Space Security |

Существуют и используются и специфические СЗИ от НСД, так и решения, выполняющие все функции системы защиты информации.

Функции, которые могут выполняться системами управления доступа к серверам, роутерам и рабочим станциям, а также системными администраторами:

- Усиленная идентификация и аутентификация пользователей - осуществляется совместно со средствами операционной системы с помощью аппаратных средств (токены, USB-ключи) при входе пользователя в систему и средств обеспечения непрерывности защиты системы. Непрерывность защиты является важной характеристикой средств защиты информации от НСД, которая выражается в отсутствии способов обращения к защищаемым ресурсам в обход системы управления доступом.
- Управление доступом на основе полномочий - функция управления доступом пользователей к конфиденциальной информации, когда каждому информационному ресурсу назначается определенная категория конфиденциальности, а каждому пользователю – уровень допуска. Доступ осуществляется по результатам сравнения уровня допуска с категорией конфиденциальности информации.
- Разграничение доступа к устройствам - обеспечивает разграничение доступа к аппаратным средствам системы с целью предотвращения несанкционированного копирования информации на отчуждаемые физические носители (диски, дискеты, USB-накопители, мобильные жесткие диски).
- Замкнутая программная среда - для каждого пользователя системы формируется определённый перечень программ, разрешенных для запуска для исключения распространения вирусов, «червей», шпионского и вредоносного ПО и использования несанкционированного ПО (чаще всего-игры).
- Контроль целостности файловой системы и ресурсов ОС, используется для слежения за неизменностью контролируемых объектов с целью защиты их от

модификации. Объектами контроля могут быть файлы, каталоги, элементы системного реестра, каждый со своим набором контролируемых параметров. При обнаружении несоответствия предусмотрены различные варианты реакции на возникающие ситуации нарушения целостности.

- Контроль аппаратной конфигурации компьютера осуществляет своевременное обнаружение изменений, реагирование на эти изменения вплоть до полной блокировки работы в случае неавторизованного изменения.
- Контроль печати конфиденциальной информации и маркировка конфиденциальных документов.
- Регистрация и учет событий в системе, таких как включение системы, вход и выход пользователей, события НСД, обращения к конфиденциальной информации, вывод конфиденциальной информации на печать и отчуждаемые носители (диски, дискеты, USB-накопители, мобильные жесткие диски).
- Тщательное удаление информации и очищение памяти после работы приложений (этому подвержены также диски, дискеты, USB-накопители, мобильные жесткие диски).

Функция регистрации и учета предназначена для фиксирования обращений к защищаемым ресурсам, что позволяет позже расследовать инциденты, связанные с утечкой или утратой информации ограниченного доступа.

И еще исключительно важная задача СЗИ от НСД – это контроль и обеспечение целостности системы. В случае если программные или аппаратные компоненты системы подвергались модификации, правильность выполнения основной функции системы может быть поставлена под сомнение, поэтому необходимо, чтобы перед стартом компоненты системы сравнивались с эталоном и, в случае обнаружения расхождений, пользователь оповещается о несанкционированной модификации системы и дальнейшая работа системы блокировалась.

Актуальность и многочисленные трудности и проблемы НСД возрастают пропорционально количеству информации, которая хранится и обрабатывается с помощью всевозможных и разноплановых информационных систем.

В современных конкурентных условиях промышленности и предпринимательства рост количества информации в информационных системах, а следственно и пользователей этих информационных систем неизбежен и возрастает как снежный ком.

Использование устаревшей схемы аутентификации на основе логина-пароля, децентрализованное, часто ручное управление учетными данными и правами доступа пользователей к ИТ- системам является предпосылками для возникновения инцидентов несанкционированного доступа к информации.

Программные и аппаратные средства позволяющие применять современные технологии аутентификации пользователей и предоставления доступа к информационным системам, а так же управление созданием и изменениями учетных записей пользователей в ИТ-системах.

Современные средства защиты информационных систем обладают большим количеством разнообразного функционала и инструментария для решения задач защиты данных от несанкционированного доступа.

Поэтому для выбора оптимального пути и способа решения задач по защите данных от несанкционированного доступа крайне важно четко осознавать приоритетные задачи и сценарии использования. Это поможет оптимально решить задачу и внедрить в компании оптимальный уровень защиты от несанкционированного доступа.

Перечислим некоторые защитные средства использующиеся в Палестине в небольшом количестве сетей[107-110].

**СЗИ Аура**

Программное средство защиты информации, использующее набор средств и способов для защиты информации и компьютера. Позволяет производить доверенную загрузку ОС, контролировать целостность ОС и доступ к

устройствам. Шифровать диски и съемные носители, достоверно уничтожать файлы. Регистрировать действия пользователя в системе и улучшать аутентификации при загрузке ОС. СЗИ Аура предоставляет механизмы защиты информации в корпоративных сетях и механизмы организации защиты информационных систем и баз данных. Является средством защиты информации от НСД.

**СЗИ от НСД Аккорд**

Программно-аппаратное средство защиты информации позволяющее производить доверенную загрузку, проверку и контроль целостности ОС. СЗИ НСД Аккорд также позволяет регистрировать действия пользователя в системе и усиливать аутентификацию при загрузке ОС. Является средством защиты информации от НСД.

**Avanpost**

Программный комплекс разворачивающий PKI инфраструктуру и организующий доступ пользователей к ИТ-системам с использованием ЭЦП. Комплект Avanpost так же предоставляет механизмы для управления учетными записями пользователей и механизмы защиты информации в корпоративных сетях.

**Biolink Idenium**

Программный комплекс позволяющий проводить биометрическую аутентификацию пользователей при входе в ОС и модифицированные приложения. Biolink Idenium является биометрическим средством защиты информации от НСД (СЗИ от НСД).

**Oracle ESSO Suite**

Программный комплекс Oracle Enterprise SSO является развитым средством для организации унифицированной аутентификации пользователей при доступе к ИТ-ресурсам компании. Oracle Enterprise SSO по оценкам западных экспертов является одним из лидеров западного рынка в сегменте программных средств защиты информации и информационных систем от несанкционированного доступа.

Система защиты информации от несанкционированного доступа **«SecretNet 5.1».**

Secret Net 5.1 – это система защиты информации на серверах и рабочих станциях от несанкционированного доступа. Функционирует под управлением ОС семейства MS Windows (Vista, XP и 2003-2010).

Таблица 1.3.3. Назначение СЗИ

| Действие | позволяет |
|---|---|
| Secret Net | предназначен для защиты информации, составляющей коммерческую или государственную тайну, или относящейся к персональным данным |
| автоматизированные системы | Приведение в соответствие законодательным требованиям и существенное упрощение процесса аттестации |
| Снижение рисков | за счет системы защиты от внутренних угроз |
| Контроль и мониторинг | позволяет повысить уровень автоматизации и сократить затраты, связанные с административными мероприятиями по безопасности |

Рассмотренные выше подходы чаще всего неприемлемы для Палестины, где распространены устаревшая аппаратура с малыми скоростями и памятью и несовершенное законодательство[107-110].

## Выводы по главе 1

1. В условиях Палестины жизненно необходима защита корпоративных и банковских сетей в условиях становления государственности.
2. Поскольку существует большая неопределенность во многих ситуациях различных угроз, проникновений и возможной защиты от них, то целесообразно применения аппарата нечеткой логики.
3. Необходимо разработать модели, методики, алгоритмы и структуры для корпоративных и банковских защищенных сетей применительно к условиям Палестины.

2. Разработка методик и алгоритмов управления безопасностью в КИТС и в интеллектуальной СППР.

2.1. Особенности палестинских КИТС и аналогии их с некоторыми предприятиями России.

В настоящее время нам поручено разработать и внедряться в корпоративную интегрированную автоматизированную информационную систему ИАИС класса систем обработки информации применительно для Палестины[107-110]. Поскольку в настоящее время внедрение в Палестине проблематично, то используем для этого российские предприятия, аналогичные по сетевой структуре палестинским (использование телефонных модемов, маршрутизаторов, малые скорости и память). Внедрение КИТС, как правило, начинается с решения задач учета. Автоматизация задач учета позволяет использовать накопленную информацию для автоматизированного решения задач управления.

Этот этап развития информационных технологий показывает готовые информационные системы управления, которые могут быть интегрированы с разработанными нами СОИ и учитывать различные и наиболее употребляемые СОА.

Тем не менее в палестинской банковской сфере свойственны специфические задачи управления, для которых нет готовых программных средств, которые нам и предстоит разрабатывать.

Первоначально к ним относятся задачи управления идентификационным процессом и своевременное обнаружение и ликвидация хакерских атак. Для их решения к настоящему времени разработаны визуальные среды, играющие роль вспомогательного инструментария, которые невозможно отнести к ИСППР.

Это состояние в области банковской связано с тем, что задачам данной сферы свойственны слабая структурированность предметной области и трудность в её формализации. Кроме того, отсутствует методология разработки проблемно ориентированных ИСППР в банковских сетях

Палестины, для создания которой необходимо разработать соответствующие методики, структуры и алгоритмы.

## 2.2. Разработка структур интеллектуальной СППР для управления безопасностью в КИТС

Используются при обнаружении и предотвращении сетевых атак методики, структуры и алгоритмы, имеющие возможность предотвращения СА и включающие в себя только лишь такие действия, как блокировка приёма/передачи тех сетевых пакетов, которые идентифицируются как пакеты, содержащиеся в атаке [26, 28, 99,100].

Мы предлагаем технологии обнаружения атак, которые позволят намного повысить существующий уровень защищенности, достигаемый известными средствами, путем изъятия НСД в реальном масштабе времени.

Такие обнаружения атак не решают проблем идентификации/аутентификации, конфиденциальности и т.п., хотя в ближайшем будущем эти механизмы будут включены в СОА.

Следует в этом случае ожидать от СОА идентификации в заданном режиме времени любых попыток использования известных уязвимостей или несанкционированного исследования внутренней сети корпораций и банков.

Контрольные органы (сетевые администраторы) должны следить за попытками перегрузки ресурсов. Они должны сигнализировать об атаке, выполнять все предписанные стратегией конкретной банковской сети действия.

Предполагаем, что структура ИСППР содержит множество функциональных компонент, производящих диагностирование состояния КИТС, идентификации атаки и автоматизирующей управляющих воздействии при изменении ситуации в КИТС.

Выявление различных вторжений (проникновений) производится на основании анализа результатов всесторонних проверок КИТС и различных внешних воздействий на нее.

Уровень технического состояния КИТС анализируются с использованием штатных средств ( в частности, системных логов, сведений об авторизации и протоколов аудита).

Среди злонамеренных внешних воздействий наибольшее внимание уделяется сетевому трафику, так как его использование лежит в основе подавляющего количества атак.

Целесообразно на первом этапе выполнить сбор первичных данных о работе КИТС [77-78], сравнить их с историей работы сети, с указанием и выявлением наиболее употребимых, злонамеренных взломщиков.

При конкретном использовании этой методики определения и идентификации СА нами разработаны модели сигнатурного и статистического анализаторов сетевого трафика, а для определения источников СА и выбора вариантов по их устранению – нечеткая интеллектуальная система (рис 2.2.1).

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 $B_j = \{b_{jk}\}_1^K$, $j = \overline{1,m}$:

$$B = B_1 \cup B_2 \cup ... \cup B_m = \bigcup_{j=1}^{m} B_j \qquad (2.2.1)$$

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 $S \subseteq B$.

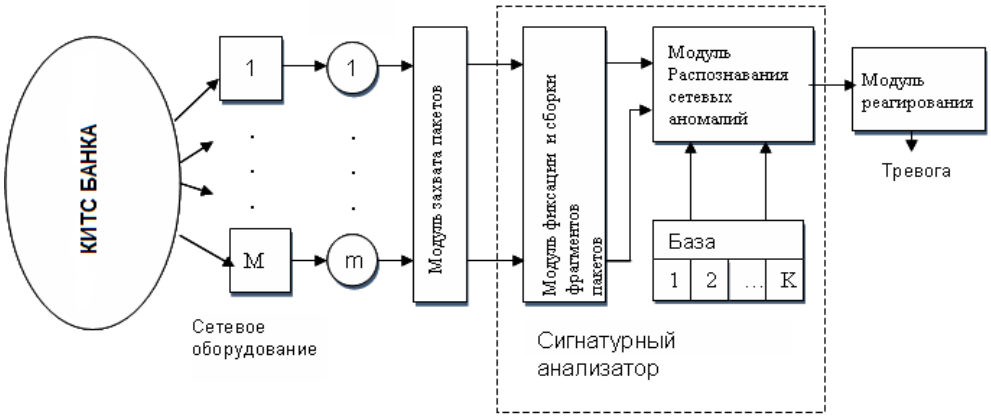



Рис.2.2.1. – Структурная схема анализатора сигнатуры

Для нашего анализатора выбираем модель на основе анализа среднего значения и среднеквадратичного отклонения параметров сетевого трафика.

Эти параметры легко получаются при диагностировании параметров сети. Такая методика, в основном, использует сравнение локальных (текущих) характеристик $Y_b$ потока пакетов с усредненными за некоторый промежуток времени (глобальными характеристиками) $y_b$.

В качестве статистических характеристик потока пакетов используются выборочное среднее значение $\xi$, выборочная дисперсия $d^2$ и критерий согласия $\chi^2$. Если же эти характеристики сильно отличаются от глобальных, проверенных временем, то делается вывод об аномальном поведении потока пакетов и вполне возможны сбои в работе всего оборудования сети(серверов, роутеров, ПК), ПО или нарушения политики безопасности, установленной заказчиком.

Статистический анализатор действует следующим образом[56,75]. Числовая величина $X_i\{x_{\min} \le X_i \le x_{\max}\}$ представляет собой некоторое событие (например, поступление нового пакета) из потока событий, произошедшее в КИТС в момент времени $t_i$, $i = \overline{1,n}$.

Множество значений характеризуется средним значением $\bar{x}$ и дисперсией $\sigma_x$ величины *X*. Для определения локальных характеристик среднее значение $\bar{x}$ будем вычислять не для всего потока из *N* событий, а только для последних *n* событий.

С этой целью используется весовая функция *F(z)* и значения локальных характеристик можно вычислять по следующей формуле:

$$W(N) = \sum_{i=1}^{N} F(t_N - t_i) f(X_i) \qquad (2.2.2)$$

В качестве весовой функции *F(z)* для нахождения *W(N)* была выбрана функция вида:

$$F_S(z) = \frac{1}{k_S} \sum_{j=1}^{S} \frac{(z/t)^j}{j!} \exp(-z/t) \qquad (2.2.3)$$

где *t* - временной интервал, на котором вычисляются локальные характеристики, $k_S$ - нормировочный коэффициент.

Для определения локальных характеристик область возможных значений *X* разбивается на *B* интервалов: $[x_{\min}, x_{\max}) \to [x_0, x_1) ... [x_{B-1}, x_B)$ и подсчитываются частоты попадания в соответствующие интервалы не для всего потока, а только для *n* последних событий. Локальные характеристики вычисляются по формулам (2.2.2) и (2.2.3).

Для выявления СА в потоке пакетов в качестве статистических характеристик используются:

– выборочное среднее числовой величины $\xi = \sum_{b=1}^{B} \tilde{x}_b Y_b$, где $\tilde{x}_b = x_{b-1} + x_b / 2$ середина интервала $[x_{b-1}, x_b)$, $Y_b$ – локальная характеристика;

– выборочная дисперсия $d^2 = \sum_{b=1}^{B} (\tilde{x}_b - \xi)^2 Y_b$;

– статистика $\chi^2 = n \sum_{b=1}^{B} (Y_b - y_b)^2 / y_b$, где $y_b$ – глобальная характеристика, определяемая на этапе настройки и обучения системы.

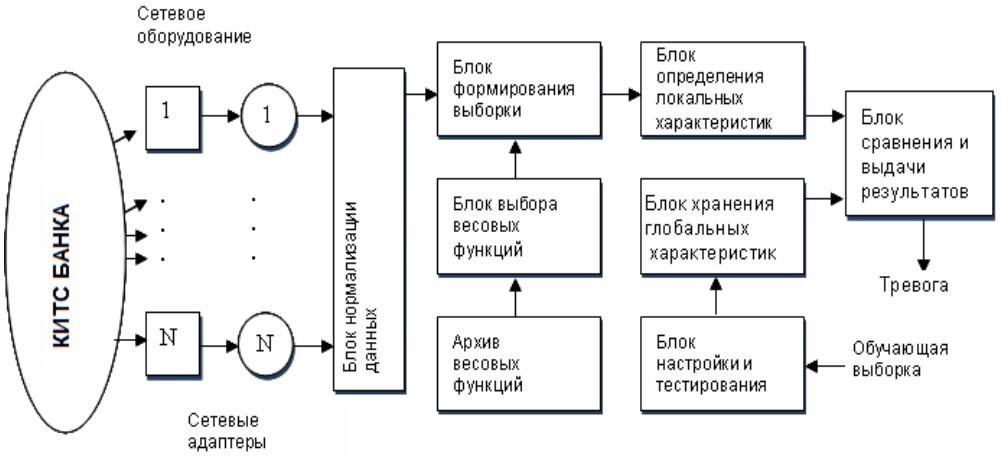



Рис 2.2.2 – Структурная схема анализатора статистики

Признаком появления СА в потоке сетевых пакетов считается сильное отклонение локальных характеристик от глобальных, проверенных временем и опытом, характеристик. при появлении СА будет превышение локальных характеристик установленных пороговых значений, предписанных заказчиком.

Для выборочного среднего таким критерием будет $\left|\xi - \overline{\xi}\right| \geq k\sigma_x$, где $\overline{\xi}$ - математическое ожидание величины $\xi$, определяемое как $\overline{\xi} = \sum_{b=1}^{B} \tilde{x}_b y_b$; параметр *k* задает границы интервала, выход, за пределы которого считается как СА.

Для выборочной дисперсии критерием выброса в потоке пакетов считается $d^2 \leq S_0^2$ где $S_0^2$ - задает нижнюю границу, выход за пределы которой воспринимается как СА. Аналогично для статистики $\chi^2 \geq \chi_0^2$, где $\chi_0^2$ - установленное пороговое значение.

При разработке экспертной ИСППР системы нами была выбрана нечеткая модель на основе метод нечеткого обобщения и анализа знаний (см. 3-ю главу). Структуру на основании ее мы и внедряли (см. приложения).

Сведения об обнаруженных проникновениях передаётся в ИСППР, где производится анализ и выработка управляющих воздействий по их устранению в случае изменения ситуация в КИТС, это позволит своевременно принять решение в интеллектуальной системе, поскольку

КИТС - сложная адаптируемая система со своей стратегией.

Комплексная ИСППР для диагностики и управление КИТС содержит набор функциональных компонент, позволяющих максимально автоматизировать и ускорить выработку управляющих воздействий при изменении ситуации в КИТС.

В состав ИСППР (рис.2.2.3) нами включено[25, 50, 98, 99]:

- подсистема мониторинга.
- блоки статистического и сигнатурного анализа.
- нечеткая интеллектуальная (экспертная) система [40].

Процесс построения НИС выполняется по следующему алгоритму:

– определение характеристик системы – задаются входные и выходные лингвистические переменные и их термы ;

– определение функций принадлежности лингвистических термов;

– формирование НБЗ, описывающей поведение объекта;

– настройка НИС путем решения задач оптимизации с использованием обучающей выборки.

–

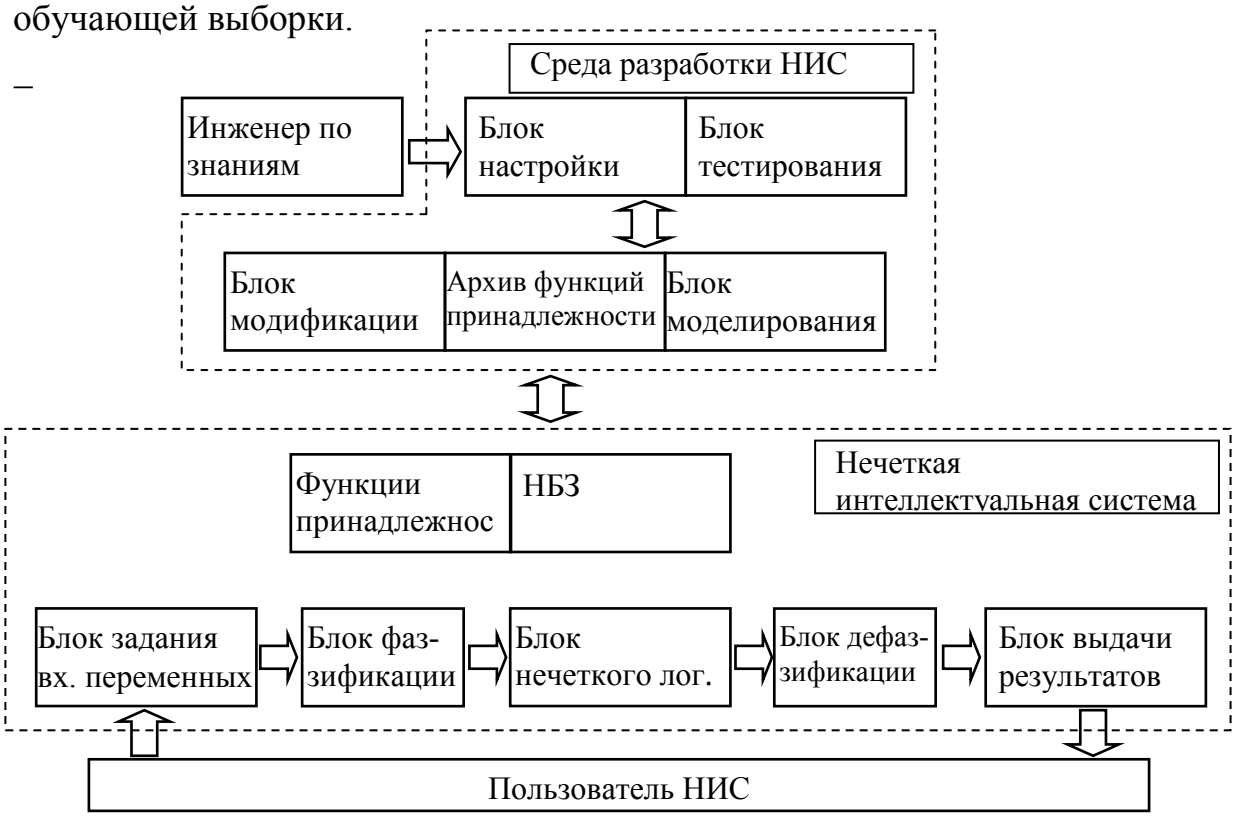



Рис.2.2.3. – Структурная схема с решениями по принципам нечеткой логики

В результате нечеткого логического вывода получаются функции принадлежности выходной переменной каждому из классов решений. В процессе моделирования инженер по знаниям и эксперт могут наблюдать за поведением моделируемого объекта в разных областях входных переменных. Настройка модели по экспериментальным данным позволяет повысить адекватность НИС.

## 2.3. Повышение уровня безопасности защиты банковской телекоммуникационной системы

Выбор состава структуры комплекса средств защиты сети предприятия(«Электроприбор», Москва). В качестве защищаемой автоматизированной биллинговой системы (АИБС) рассматривалась система низшего уровня, состоящая из ПК, сервера и аппаратуры передачи данных.

Цели злоумышленника, перечень угроз информации соответствуют рассмотренным выше. Наибольшую опасность с точки зрения наносимого ущерба носят угрозы, связанные с нарушением процесса функционирования системы, что требует очень целенаправленного большего внимания на их устранение.

В качестве, заданных заказчиком, характеристик средств защиты, на основании которых осуществлялся их выбор, использовались стоимость конкретного средства и вероятность успешного функционирования по нейтрализации соответствующей угрозы. Моделирование проводилось для различных значений ограничения на стоимость системы защиты в использованием стандартного ПО на ПК.

Рассматривался подбор комплекса защитных средств, нейтрализующих цель №3 и все цели злоумышленника. Предположительно атака осуществляется четырехкратным повторением комплекса угроз (к=4). Время решения программы составило 40 с. Результаты представлены в табл.2.3.1 и на рис.(2.3.1-2).

Таблица 2.3.

| Подбор комплекса защитных средств, нейтрализующих цель №3 | | | | Подбор комплекса защитных средств, нейтрализующих все цели | | | |
|---|---|---|---|---|---|---|---|
| **№ набора СЗ** | **Номера средств защиты набора** | **Общая стоимость комплекса средств защиты** | **Вероятность достижения цели** | **№ варианта** | **Номера средств защиты набора** | **Общая стоимость комплекса средств защиты** | **Вероятность реализации злоумышленником всех целей** |
| 1 | 3, 4, 6 | 2195,00 | 4,39E-01 | 1 | 1, 3, 5, 7, 8 | 6848,00 | 8,41E-04 |
| 2 | 3, 6, 7 | 3434,00 | 1,22E-02 | 2 | 1, 3, 7, 8, 9 | 6318,00 | 3,75E-03 |
| 3 | 3, 6, 5 | 3315,00 | 4,38E-02 | 3 | 1, 3, 4, 7, 8 | 6927,00 | 4,03E-04 |
| 4 | 3, 6 | 1815,00 | 8,21E-01 | 4 | 1, 6, 10 | 3911,00 | 6,11E-03 |
| 5 | 3, 6, 8 | 2695,00 | 8,31E-02 | 5 | 1, 3, 5, 6 | 6624,00 | 3,88E-04 |
| 6 | 3, 6, 9 | 1784,00 | 4,52E-01 | 6 | 2, 3, 5, 7, 8 | 3339,00 | 1,92E-03 |
| 7 | 3, 7, 8 | 2468,00 | 2,11E-01 | 7 | 2, 3, 7, 8, 9 | 3035,00 | 1,94E-02 |
| 8 | 3, 4, 7, 8 | 3201,00 | 1,21E-02 | 8 | 2, 3, 4, 7, 8 | 2939,00 | 1,22E-02 |
| 9 | 3, 5, 7, 8 | 4211,00 | 2,62E-02 | 9 | 2, 6, 10 | 2011,00 | 5,08E-02 |
| 10 | 3, 7, 8, 9 | 2555,00 | 1,39E-01 | 10 | 2, 3, 5, 6 | 5252,00 | 8,82E-03 |
| 11 | 3,4,7,8, 9 | 3182,00 | 6,34E-03 | 11 | 3, 5, 7, 8 | 3989,00 | 6,01E-03 |
| | | | | 12 | 3, 5, 7, 8, 9 | 4134,00 | 9,22E-03 |
| | | | | 13 | 3, 4, 5, 7, 8 | 3987,00 | 1,23E-03 |
| | | | | 14 | 3, 5, 6 | 3135,00 | 7,01E-03 |


Рис. 2.3.1. Влияние стоимости комплекса защиты на вероятность достижения цели злоумышленником


Рис.2.3.2. Влияние стоимости комплекса защиты на вероятность достижения цели злоумышленником всех целей

Из результатов экспериментов видно, что с увеличением объема ассигнований на средства защиты в целом вероятность реализации злоумышленником всех целей значительно снижается. Причем, данная зависимость носит явно выраженный экспоненциальный с отрицательным коэффициентом характер. Это общая тенденция. Тем не менее в отдельных случаях стоимость средств не показатель снижения вероятности реализации злоумышленником всех целей, например, включение в состав комплекса дорогого средства защиты №7, нейтрализующего многие из угроз, нежелательно из-за низкой эффективности блокирования этих угроз. «Выигрывает», как правило, комплекс, состоящий из многих недорогих средств защиты, специализирующихся на угрозах определенного вида.

Управление безопасностью в условиях многократно повторяемых угроз (длительных атаках). Определим ожидаемой суммы потерь от реализации угроз серверу АИБС.

Исходные данные.

Имеется сервер АИБС, по отношению к которому рассматриваются пять уязвимостей с вероятностями 0.2, 0.2, 0.1, 0.05 и 0.45. Первую из них могут использовать две угрозы с вероятностями 0.35 и 0.65, вторую — три (0.4, 0.2, 0.4), третью — две (0.3, 0.7), Четвертую — три (0.25, 0.25, 0.5), пятую — две (0.3, 0.7). Комплекс средств защиты (шифрования Экраны, Антивирусные, удаления файлов). Значения недостатков защитных механизмов оцениваются как 0.3, 0.4, 0.4, 0.1, 0.25, 0.25, 0.15, 0.25, 0.4, 0.4, 0.2, 0.15. Сколько общий остаточный риск. Критичность сервера (Sun Fire V490) оценим как 1 и стоимость 10964 $.

Определим: величину риска, общий остаточный риск, ожидаемую сумму потерь и ожидаемая сумма затрат система, уровень риска. Вероятность реализации злоумышленником всех целей, вероятность успешно комплекс средств защиты.

Для решения используем разработанный нами алгоритм:

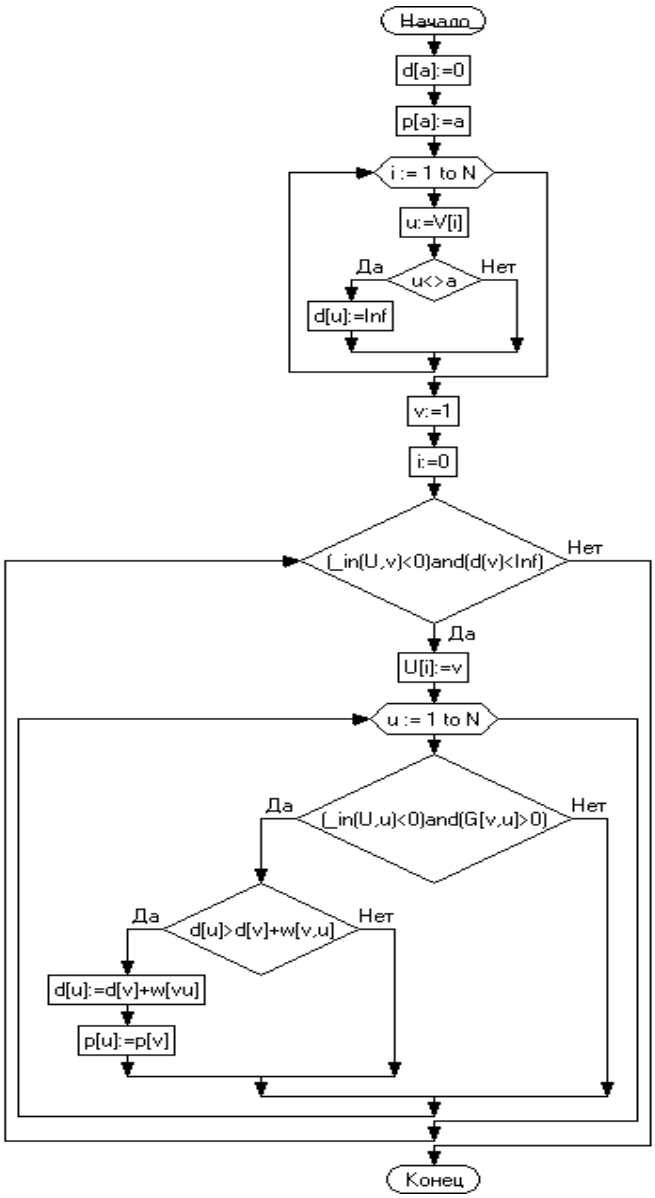



Рис 2.3.3. Структура алгоритма для уязвимостей с заданными заказчиком затратами.

==========

КОНСОЛЬНОЕ ПРИЛОЖЕНИЕ. Обзор проекта asd

==========

Это приложение asd создано автоматически с помощью мастера приложений.

Здесь приведены краткие сведения о содержимом каждого из файлов, использованных

при создании приложения asd.

asd.vcxproj

Основной файл проекта VC++, автоматически создаваемый с помощью мастера

приложений.

Он содержит данные о версии языка Visual C++, использованной для

создания
файла, а также сведения о платформах, настройках и свойствах проекта,
выбранных с помощью мастера приложений.
asd.vcxproj.filters
Это файл фильтров для проектов VC++, созданный с помощью мастера
приложений.
Он содержит сведения о сопоставлениях между файлами в вашем проекте и
фильтрами. Эти сопоставления используются в среде IDE для группировки
файлов с одинаковыми расширениями в одном узле (например файлы ".cpp"
сопоставляются с фильтром "Исходные файлы").

asd.cpp
Это основной исходный файл приложения.
////////////////////////////////////////////////////////////////////////////
Другие стандартные файлы:
StdAfx.h, StdAfx.cpp
Эти файлы используются для построения файла предкомпилированного заголовка
(PCH) с именем asd.pch и файла предкомпилированных типов
с именем StdAfx.obj.
////////////////////////////////////////////////////////////////////////////
Общие замечания:
С помощью комментариев «TODO:» в мастере приложений обозначаются фрагменты
исходного кода, которые необходимо дополнить или изменить.
////////////////////////////////////////////////////////////////////////////
```
#include "stdafx.h"
#include <stdio.h>
#include <iostream>
#include <string>
#include <cstdlib>
#include <math.h>
using namespace std;
int main()
{
 int a;
 float l[202];
 float I[202];
 float L=0;
 l[0]=0.001;
```

```
 for (int i=0;i<200;i++)
 {
        l[i+1]=l[i]+0.001;
        L=L+l[i];
        //cout<<L<<endl;
 }
 cout<<"L="<<L<<endl;

 for (int i=0;i<200;i++)
 {
        l[i+1]=l[i]+0.001;
        I[i]=-(l[i]/L)*log(L/l[i])-(1-l[i]/L)*log(1/(1-l[i]/L));
        cout<<i+1<<") "<<"I[i]="<<I[i]<<"    l["<<i<<"]="<<l[i]<<endl;
 }
 system ("pause");
 return 0;
}
// stdafx.cpp: исходный файл, содержащий только стандартные включаемые модули
// asd.pch будет предкомпилированным заголовком
// stdafx.obj будет содержать предварительно откомпилированные сведения о типе
#include "stdafx.h"
// TODO: Установите ссылки на любые требующиеся дополнительные заголовки в файле STDAFX.H
// , а не в данном файле
// stdafx.h: включаемый файл для стандартных системных включаемых файлов
// или включаемых файлов для конкретного проекта, которые часто используются, но
// не часто изменяются
//
#pragma once
#include "targetver.h"
#include <stdio.h>
#include <tchar.h>
// TODO: Установите здесь ссылки на дополнительные заголовки, требующиеся для программы
#pragma once
// Включение SDKDDKVer.h обеспечивает определение самой последней доступной платформы Window
// Если требуется выполнить построение приложения для предыдущей версии Windows, включите WinSDKVer.h и
// задайте для макроса _WIN32_WINNT значение поддерживаемой
```

платформы перед включением SDKDDKVer.h.

#include <SDKDDKVer.h>

Решение задачи:

1. Множество уязвимости.

Таблица 2.3.2. Различные уязвимости.

| № | Класс уязвимости | Краткое описание уязвимости | Конкретный пример (если имеется) | Вероятность уязвимости |
|---|---|---|---|---|
| **1** | Программное обеспечение | Небрежно написанные приложения | Использование межузловых сценариев | 0.2 |
| **2** | Программное обеспечение | Сознательно созданные уязвимости | «Черные ходы», оставленные производителями для управления или восстановления систем | 0.2 |
| **3** | Программное обеспечение | Сознательно созданные уязвимости | Программы-шпионы, например клавиатурные шпионы | 0.1 |
| **4** | Программное обеспечение | Сознательно созданные уязвимости | Троянские программы | 0.05 |
| **5** | Программное обеспечение | Ошибки в конфигурации | Подготовка к работе вручную, приводящая к несогласованным конфигурациям | 0.45 |

Таблица 2.3.3. Угрозы серверам в сетях.

| № п\п | Наименование, источник | Уровень вероятности | Вероятность угрозы | $P_{уя}$ |
|---|---|---|---|---|
| **1** | Кража пароля или подбор пароля | Низкая | 0.35 | 0.2 |
| **2** | Внедрение программ-закладок | Высокая | 0.65 | |
| **3** | Заражение элементов вирусами | Низкая | 0.4 | 0.2 |
| **4** | Прослушивание информационного трафика | Очень низкая | 0.2 | |
| **5** | Сборка "мусора"(Вн. и внш..) | Низкая | 0.4 | |
| **6** | Сканирование носителей информации | Низкая | 0.3 | 0,1 |
| **7** | Запуск программы в качестве системной | Высокая | 0.7 | |
| **8** | Подмена динамически загружаемой библиотеки | Очень низкая | 0.25 | 0,05 |
| **9** | Модификация кода или данных подсистемы защиты ОС. | Очень низкая | 0.25 | |
| **10** | Захват ресурсов. (Вн. и внш..) | Средняя | 0.5 | |
| **11** | Бомбард. запросами. | Низкая | 0.3 | 0,45 |
| **12** | Нарушение функционирования. | Высокая | 0.7 | |

Таблица 2.3.4.Комплексный подбор средств защиты.

| № | Наименование | Стоимость | Эффективность | |
|---|---|---|---|---|
| **2** | Средства шифрования отдельных сообщений (почты, передаваемых файлов, блоков) | 250 | Высокая | 0,9 |
| **5** | Межсетевые экраны | От 1500 до 40000 | Средняя | 0,45 |
| **9** | Антивирусные средства | От 90 и выше (на 1 польз.) | Низкая | 0,3 |
| **10** | Средства гарантированного удаления файлов | 30 | Высокая | 0,8 |

Таблица 2.3.5. Значения риска.

| $P_{уя}$ | 0.2 | | 0.25 | | | 0.1 | | 0.05 | | | 0.45 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $P_{уг}$ | 0.35 | 0.65 | 0.4 | 0.2 | 0.4 | 0.3 | 0.7 | 0.25 | 0.25 | 0.5 | 0.3 | 0.7 |
| P*риск* | 0.035 | 0.065 | 0.02 | 0.01 | 0.02 | 0.06 | 0.14 | 0.0375 | 0.0375 | 0.125 | 0.054 | 0.126 |
| **Н** защ | 0.3 | 0.4 | 0.4 | 0.1 | 0.25 | 0.25 | 0.15 | 0.25 | 0.4 | 0.4 | 0.2 | 0.15 |
| Уровень риска | **Н** | **С** | **Н** | **Н** | **Н** | **С** | **С** | **Н** | **Н** | **С** | **С** | **С** |

Общий остаточный риск составит: $O_{k1(5,9,11)}$ = 0.24

Таблица 2.3.6. Результаты с защитой с шифрованием.

| **Повторная** | **Остаточный риск** | **Стоимость** | **Вероятность реализации злоумышленником** |
|---|---|---|---|
| K=1 | 0.239375 | 21120 | 0,000038 |
| K=2 | 0,42144 | 21120 | 0,0000746 |
| K=4 | 0,88796 | 21120 | 0,000303 |
| K=6 | 0,99984 | 21120 | 0,001225 |
| K=8 | 0,9999 | 21120 | 0,0049 |
| K=10 | 0,99999 | 21120 | 0,00967 |
| K=12 | 0,999999 | 21120 | 0,0397 |
| K=14 | 0,999999 | 21120 | 0,156 |
| K=16 | 0,999999 | 21120 | 0,615 |
| K=18 | 0,999999 | 21120 | 0,9408 |

Общий остаточный риск составит: $\mathbf{O}_{k\,(1,3,5,7,8)}$ = 0.0945 (**нови**)

Таблица 2.3.7. Результаты с разработанной нами защитой

| **Повторная** | **Остаточный риск** | **Стоимость** | **Вероятность реализации злоумышленником** |
|---|---|---|---|
| k=1 | 0.0945 | 6939 | 5,6E-08 |
| k=2 | 0.1954 | 6939 | 1,12E-07 |
| k=4 | 0.29635 | 6939 | 3,87E-10 |

| | | | |
|---|---|---|---|
| k=6 | 0.34235 | 6939 | 1,55E-09 |
| k=8 | 0.45854 | 6939 | 9,91E-08 |
| k=9 | 0.492 | 6939 | 1,98E-07 |
| k=10 | 0.524 | 6939 | 3,96E-07 |
| k=11 | 0.686 | 6939 | 7,93E-07 |
| k=12 | 0.752 | 6939 | 1,59E-06 |
| k=14 | 0.768 | 6939 | 6,34E-06 |
| k=16 | 0.823 | 6939 | 2,54E-05 |
| k=21 | 0.912 | 6939 | 0,0008 |
| k=23 | 0.924 | 6939 | 0,0033 |
| k=29 | 0.9962145 | 6939 | 0,0129 |
| k=31 | 0.999 | 6939 | 5,09E-02 |
| k=37 | 0.999 | 6939 | 0,656 |

Таблица 2.3.8. Потери средств защиты в сравнении с разработанных нами

| № | Критичность | Стоимость | $O_{k\ (2,5,9,10)}$ | | Потерь | | $O_{k\ (1,3,5,7,8)}$ | | Потерь | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | K=1 | K=16 | K=1 | K=16 | K=1 | K=40 | K=1 | K=8 |
| **1** | 0.8 | 7520$ | 0.2393 | 1 | 1220,08$ | 6016$ | 0.0945 | 1 | 568,5 $ | 6016$ |
| **2** | 0.85 | 8360$ | | | 1700,99$ | 7106$ | | | 671,6 $ | 7106$ |
| **3** | 0.9 | 9720$ | | | 2094,05$ | 8748$ | | | 826,7 $ | 8748$ |
| **4** | 1 | 10964$ | | | 2624,5$ | 10964$ | | | 1036,1 $ | 10964$ |
| **5** | 1 | 11524$ | | | 2758,55$ | 11524$ | | | 1089,01$ | 11524$ |
| **6** | 0.8 | 3544$ | | | 678,7$ | 2835,2$ | | | 334,9$ | 2835,2$ |
| **7** | 0.7 | 5740$ | | | 961,9$ | 4018$ | | | 379,7$ | 4018$ |
| **8** | 0.6 | 3884$ | | | 557,9$ | 2330,4$ | | | 220,3 $ | 2330,4$ |


Рис 2.3.4. Отличие реализации злоумышленником для известного комплекса средств защиты завода «Электроприбор»(г. Москва) и нового, предложенного и внедренного нами, комплекса сервера АИБС

Анализ результатов.

В результате моделирования выявлено, что существующий комплекс средств защиты информации сервера АБС в условии даже кратковременных атак не обеспечивает требуемый уровень информационной безопасности – цели злоумышленника будут практически (на 70%) реализованы двенадцатикратным повторением однотипных угроз атаки. За это время подобрать дополнительные защитные механизмы администратору не всегда удастся, а значит атака будет пропущена. Предлагаемый вариант введения дополнительных механизмов защиты позволит «удержать» атаку значительно дольше. Показана практическая реализация процедуры управления безопасностью, позволяющая в рамках выделяемых средств оптимальным образом обеспечить защиту охраняемых данных.

Результаты для информационных параметров КИТС. Подсистема статистического анализатора обеспечивает анализ данных методами математической статистики.

Статистический анализатор представляет собой совокупность трех основных блоков: базы данных, блока прогнозных расчетов и блока аналитических расчетов (рис.2.3.5).

Данные анализа поступают из базы данных ПК, куда предварительно заносились из раннего опыта, или вводятся вручную. Блок прогнозных расчетов включает с возможными, различными моделями следующие действия и критерии (табл.2.3.9.):

Таблица 2.3.9. Модели и критерии

| Модели | Действие | Критерии, расчеты |
|---|---|---|
| модель временных рядов | подбирает конкретный состав из выбранной функции, производит сглаживание исходного динамического ряда, строит прогноз на основе выбранного тренда | Экспертная оценка |
| модель “парная регрессия” | задает уравнения линейной и нелинейной регрессии, оценивает их статистические характеристики, производит подбор оптимальной формы связи по максимальному корреляционному отношению | Экспертная оценка |
| Оценка коэффициентов регрессии и уравнения | четыре модели многомерного факторного анализа, в частности модель кластерного анализа, обеспечивающую кластеризацию исходных данных | критерий Фишера |
| модель одно и двухфакторного дисперсионного анализа | определения степени влияния того или иного фактора на результативный фактор | критерий Фишера |
| модель компонентного анализа | позволяет среди множества факторов выявить главные, а также малоинформативные факторы многомерного статистического анализа | Экспертная оценка |
| модель корреляционного анализа | позволяет получить корреляционную матрицу, среднее статистическое отклонение, значения $t$ - статистика | Экспертная оценка |
| Комплексный анализ | Использует экспертные оценки и описания по всем массивам | Экспертная оценка |

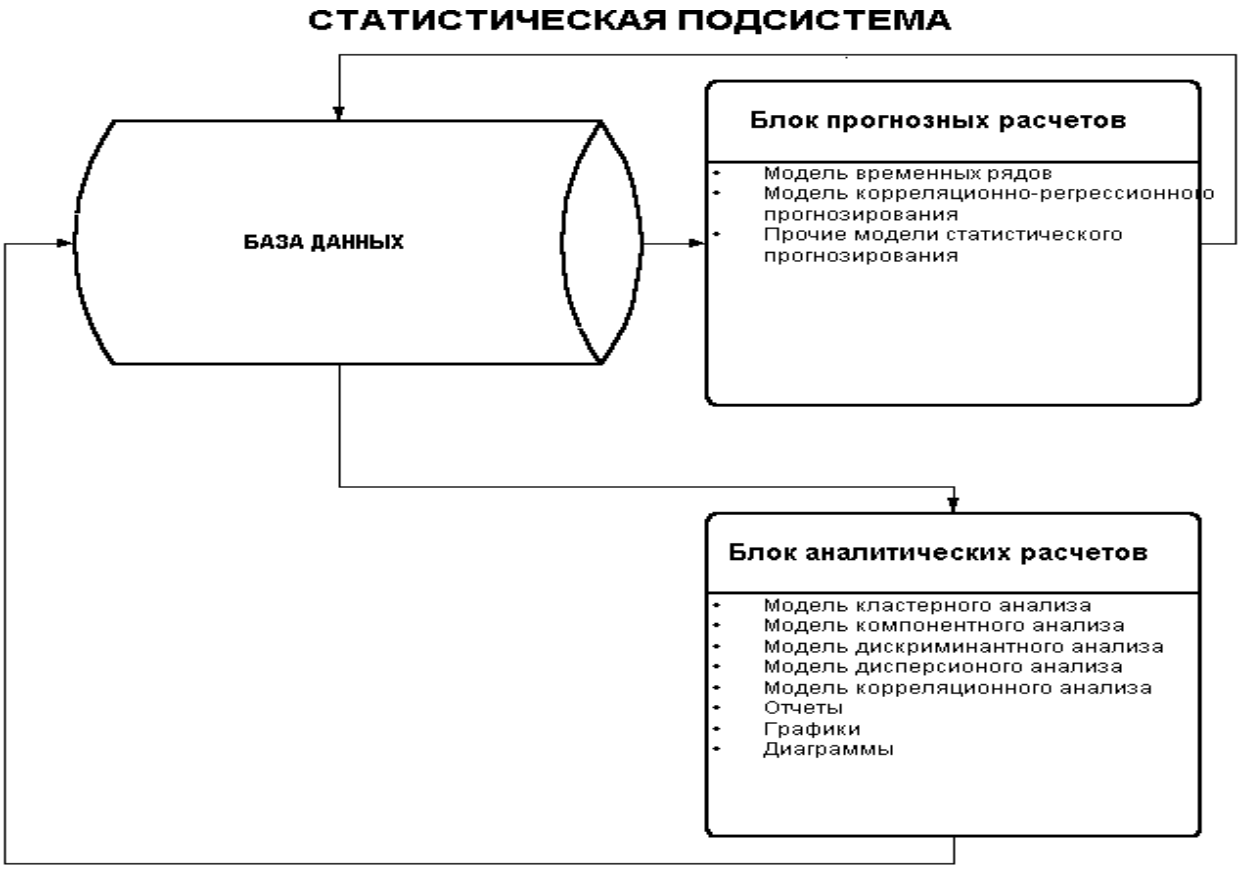



Рис.2.3.5. Схема анализатора статистики

На рис.(2.3.6 -8) приведены примеры расчетных реализаций статистического анализатора. Отсюда расчетные параметры поступают в ИСППР, в этом или другом ПК, для нечетких анализов и прогнозов и оценок.

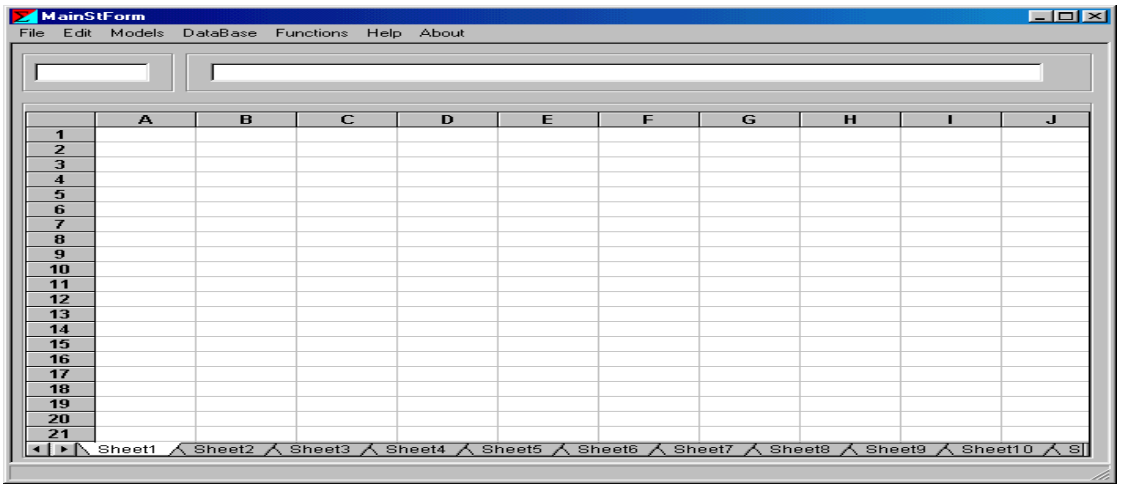



Рис.2.3.6. Экран статистической подсистемы

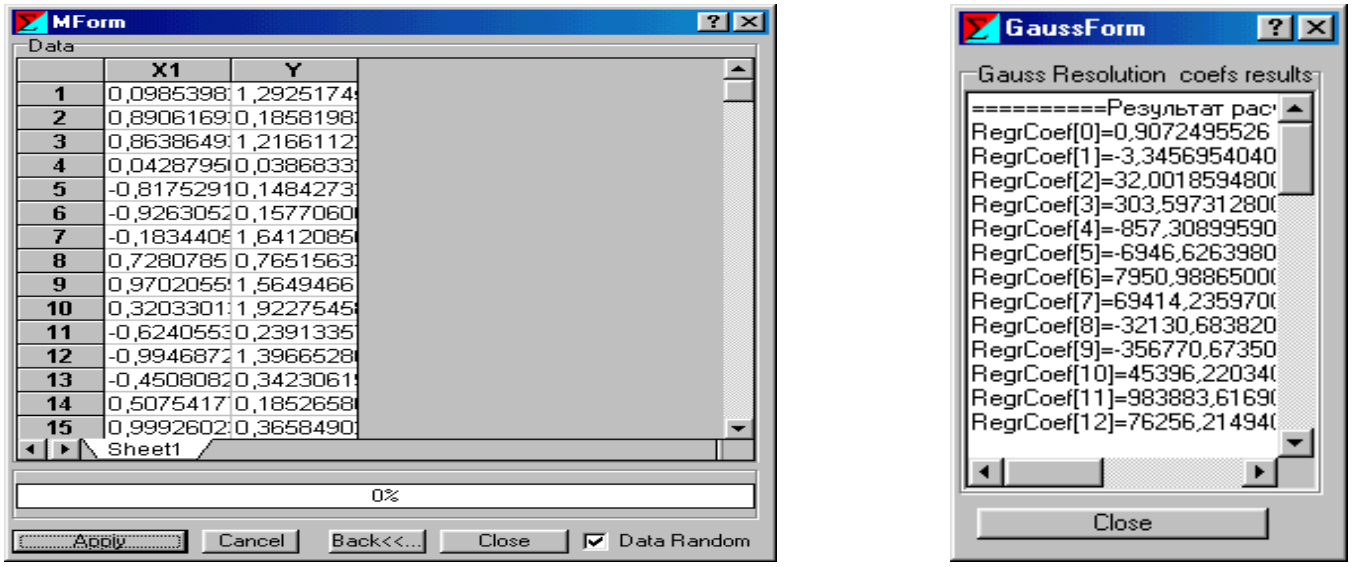



Рис. 2.3.7. Коэффициенты регрессии (см. табл.2.3.9).

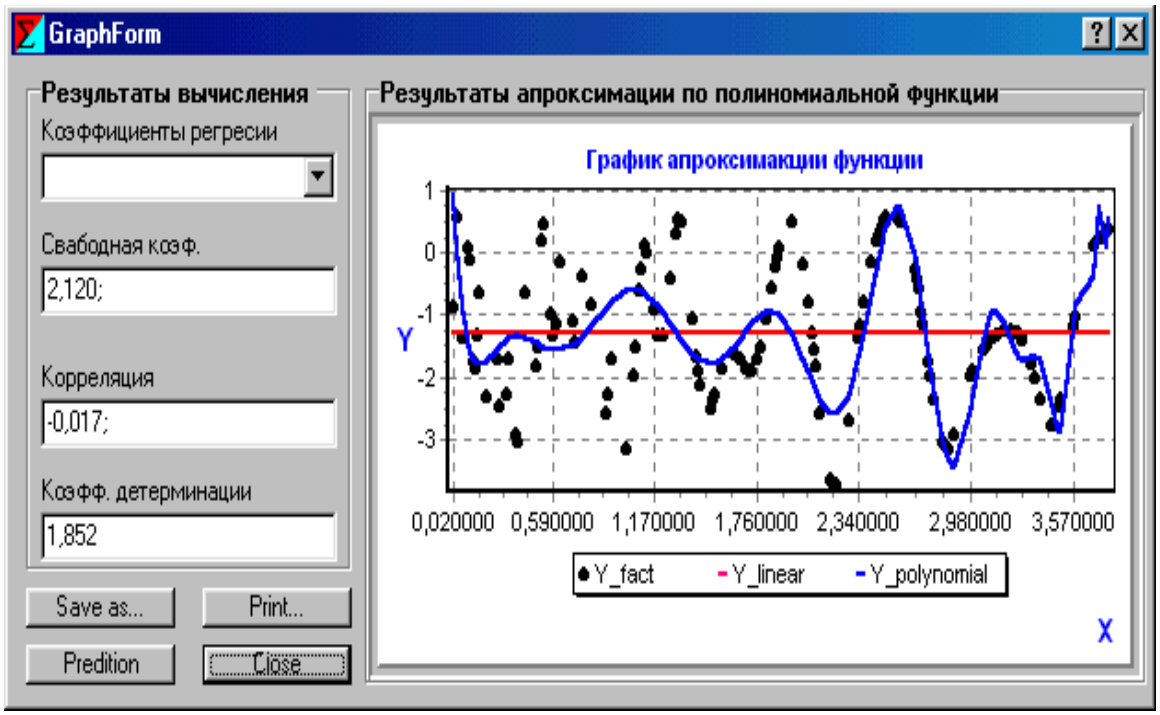
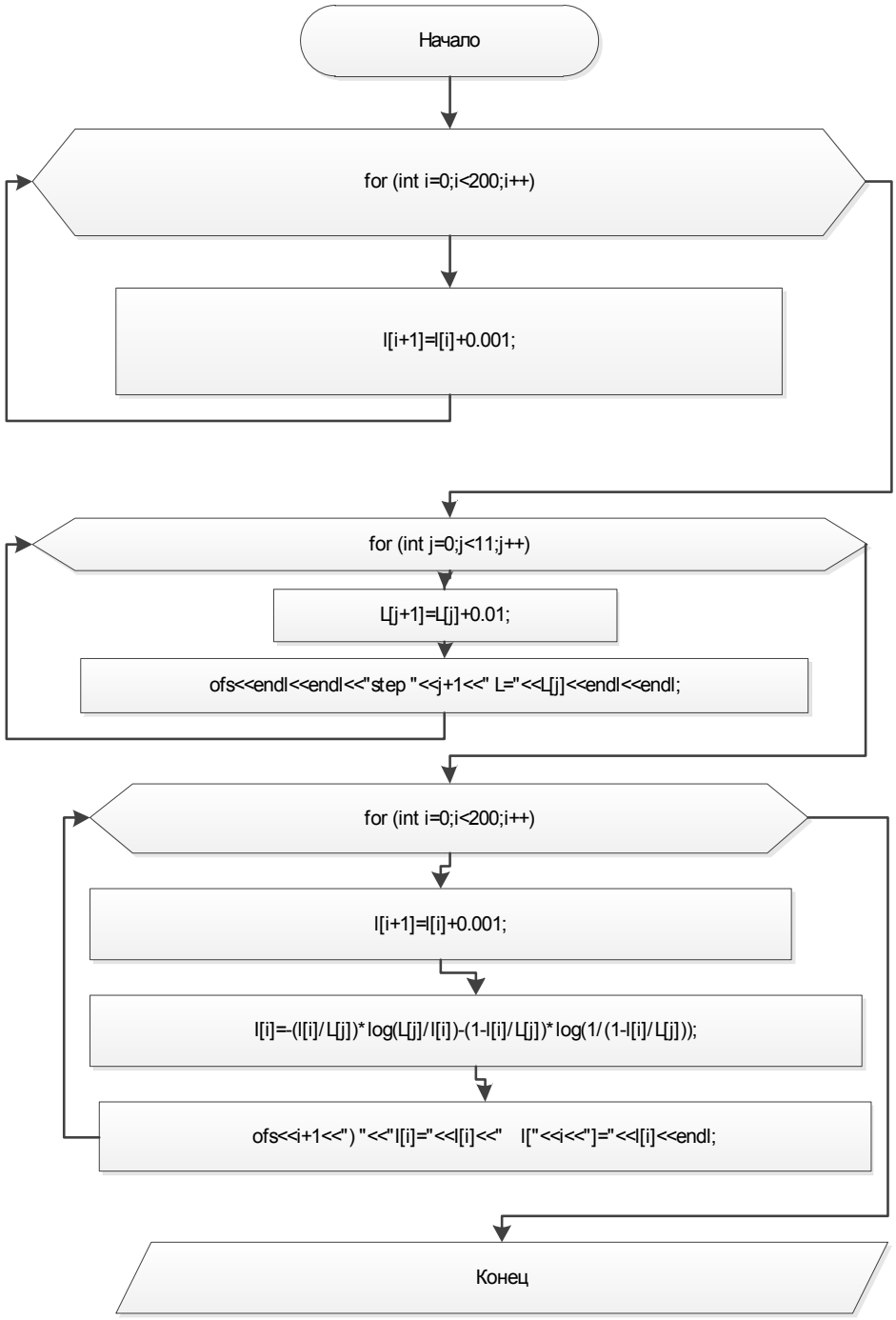



Рис. 2.3.8. Аппроксимация данных по полиномиальной функции и линейной функции (прямая линия)

Для быстрого и четкого определения вероятностных характеристик и улучшения экспертных оценок в ИСППР нами разработан алгоритм и программа и получены с ее помощью числовые данные, которые мы используем для анализа устойчивости результатов и возможности их

использования в инженерных расчетах при проектировании и эксплуатационной защиты КИТС.




по каждой большой лямбде

```
#include "stdafx.h"
#include <stdio.h>
#include <iostream>
#include <string>
#include <cstdlib>
#include <fstream>
#include <math.h>
using namespace std;
```

```
int main()
{
	int a;
	float l[203];
	float I[203];
	float L[12];
	l[0]=0.001;
	L[0]=0.9;
	std::ofstream ofs("tablica.txt");

	for (int i=0;i<200;i++)
	{
		l[i+1]=l[i]+0.001;
	}

	for (int j=0;j<11;j++)
	{
		L[j+1]=L[j]+0.01;
		ofs<<endl<<endl<<"step "<<j+1<<" L="<<L[j]<<endl<<endl;
		for (int i=0;i<200;i++)
		{
			l[i+1]=l[i]+0.001;
			I[i]=-(l[i]/L[j])*log(L[j]/l[i])-(1-l[i]/L[j])*log(1/(1-l[i]/L[j]));
			ofs<<i+1<<") "<<"I[i]="<<I[i]<<"    l["<<i<<"]="<<l[i]<<endl;
		}
	}
	system ("pause");
	ofs.close();
	return 0;

	.....................................................................
	сумма лямбд больших данных на листе
#include "stdafx.h"
#include <stdio.h>
#include <iostream>
#include <string>
#include <cstdlib>
```

step 1 L=0.9

1) I[i]=-0.00866871  l[0]=0.001
2) I[i]=-0.0157959  l[1]=0.002
3) I[i]=-0.0223404  l[2]=0.003
4) I[i]=-0.0285061  l[3]=0.004
5) I[i]=-0.0343899  l[4]=0.005
6) I[i]=-0.0400486  l[5]=0.006
7) I[i]=-0.0455201  l[6]=0.007
8) I[i]=-0.0508311  l[7]=0.008
9) I[i]=-0.0560015  l[8]=0.009
10) I[i]=-0.061047  l[9]=0.01
11) I[i]=-0.06598  l[10]=0.011
12) I[i]=-0.0708106  l[11]=0.012
13) I[i]=-0.0755472  l[12]=0.013
14) I[i]=-0.0801969  l[13]=0.014
15) I[i]=-0.0847661  l[14]=0.015
16) I[i]=-0.0892598  l[15]=0.016
17) I[i]=-0.0936828  l[16]=0.017
18) I[i]=-0.0980391  l[17]=0.018
19) I[i]=-0.102332  l[18]=0.019
20) I[i]=-0.106566  l[19]=0.02
21) I[i]=-0.110743  l[20]=0.021
22) I[i]=-0.114865  l[21]=0.022
23) I[i]=-0.118936  l[22]=0.023
24) I[i]=-0.122957  l[23]=0.024
25) I[i]=-0.126931  l[24]=0.025
26) I[i]=-0.130858  l[25]=0.026

27) I[i]=-0.134742 l[26]=0.027
28) I[i]=-0.138584 l[27]=0.028
29) I[i]=-0.142384 l[28]=0.029
30) I[i]=-0.146145 l[29]=0.03
31) I[i]=-0.149867 l[30]=0.031
32) I[i]=-0.153553 l[31]=0.032
33) I[i]=-0.157202 l[32]=0.033
34) I[i]=-0.160816 l[33]=0.034
35) I[i]=-0.164397 l[34]=0.035
36) I[i]=-0.167944 l[35]=0.036
37) I[i]=-0.171459 l[36]=0.037
38) I[i]=-0.174943 l[37]=0.038
39) I[i]=-0.178397 l[38]=0.039
40) I[i]=-0.18182 l[39]=0.04
41) I[i]=-0.185215 l[40]=0.041
42) I[i]=-0.188581 l[41]=0.042
43) I[i]=-0.191919 l[42]=0.043
44) I[i]=-0.195231 l[43]=0.044
45) I[i]=-0.198515 l[44]=0.045

Полная выкладка расчетов приведена в приложении 2.3.1.

Из приведенных рисунков и таблиц и числовых параметров хорошо заметны устойчивость результатов, что приводит к оценке, удовлетворяющей по точностным характеристикам заказчиков (см. приложения).

## Выводы по главе 2

1. Разработана структура ИСППР для диагностики состояния КИТС, реализующая проведение сигнатурного и статистического анализа сетевого трафика и работу НИС реагирования на нештатные злонамеренные сетевые ситуации.

2. Результаты экспериментальной проверки разработанных моделей и алгоритмов оптимизации состава средств защиты и управления безопасностью на основе анализа рисков показали их хорошую работоспособность и практическую значимость, подкрепленных мнением заказчиков.

3. Нами выработаны конкретные рекомендации и предложения по проектированию новых и усовершенствованию существующих систем защиты информации в КИТС.

3. Защита корпоративных и банковских сетей.

3.1. Построение структуры для защиты сети от НСД.

Для цели зашиты сети от несанкционированного доступа нами [99] создается подсистема, позволяющая решать задачи:

-распределение маршрутизатора: Устройство локализует маршрутизаторы в узлах графа пересечения канала для общей топологической структуры системного уровня. Ребра различных ядер формируют ребра графа пересечения канала. Пересечение двух ребер в углах ядер обозначает вершины в графе.

-Ядро к преобразованию маршрутизатора: Как следующий шаг, устройство соединяет каждое ядро с одним из маршрутизаторов на его четырех ребрах. Для этого имеется оптимальный алгоритм для ядра в стадии преобразования маршрутизатора.

-Генерирование маршрута и синтез топологии: Затем устройство генерирует маршруты для каждого из путей. Объединение маршрутов для всех путей завершает формирование полной топологии сети. Представлен алгоритм приближения, который маршрутизирует пути и синтезирует топологию таким образом, чтобы расход энергии был минимален, и чтобы необходимое число маршрутизаторов было бы максимум в 2 раза больше, чем в оптимальном решении[23-28, 99].

-Слияние маршрутизатора: предпоследний шаг в стадии синтеза соединяет близко находящиеся маршрутизаторы в один маршрутизатор, при условии, что ограничения длины канала передачи данных не нарушены.

-Анализ зависания: заключительный этап в потоке синтеза анализирует произведенную топологию на потенциальные зависания. Поскольку маршруты различных путей определены в стадии проектирования, можно обнаружить и уменьшить потенциальные зависания в синтезируемой структуре.

На рис.3.1.1 показано схематично проектирование специализированного приложения.

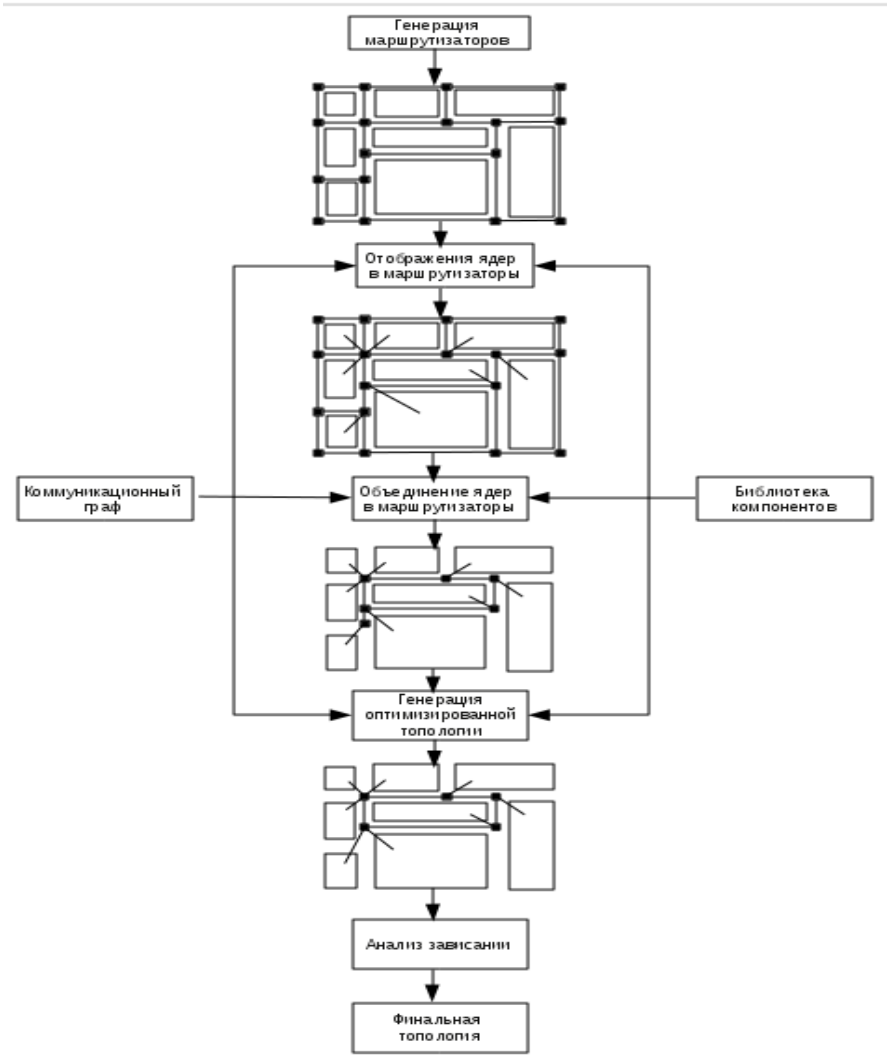



Рис.3.1.1.

В качестве среды программирования для реализации подсистемы проектирования была выбрана система инженерных и научных вычислений MATLAB. А так же использовался язык программирования C++.

Определяющими при выборе MATLAB было[99]:

- динамический обмен данными между различными приложениями на основе DDE интерфейса;
- встроенная реализация матричных и арифметико-логических операций над объектами произвольной размерности;
- использование объектно-ориентированного подхода;

- трансляция кода среды MATLAB в код языков программирования высокого уровня типа C, C++, FORTRAN;
- возможность формирования динамически подключаемых библиотек (DLL).

Система MATLAB позволяет решать многие вычислительные задачи, связанные с векторно-матричными формулировками, существенно сокращая время, которое потребовалось бы для программирования на скалярных языках (C, Pascal и т.п.). Кроме того, она предоставляет широкие возможности разработки и реализации профессиональных приложений, обеспечивает гибкую связь с другими программами.

Комплекс программ подсистемы САПР проектирования состоит из основной вызываемой программы и ряда дополнительных подпрограмм, которые реализованы в виде M-файлов. Структура любой функции, оформленной как M-файл, включает четыре обязательных раздела:

- строку определения функции, которая задает имя, количество и порядок следования входных и выходных аргументов;
- первую строку комментария, которая определяет назначение функции;
- комментарий, определяющий спецификацию функции;
- тело функции - программный код, который реализует вычисления и присваивает значения выходным аргументам.

Разработанный программный комплекс представляет собой подсистему САПР, реализованную по агрегатному принципу на основе открытой архитектуры, что позволяет легко осуществлять ее наращивание. Структура комплекса представлена на рис. 3.1.2. Выбор данной концепции при создании подсистемы был сделан, исходя из критерия универсальности и легкости модификации и дополнения комплекса каждым конечным пользователем при решении своих задач. При эксплуатации подсистемы в комплексном режиме необходимо подключение дополнительных модулей, осуществляющих импорт данных из файла отчета внешнего пакета схемотехнического моделирования. Данное обстоятельство объясняется тем фактом, что все пакеты, присутствующие на рынке САПР в настоящее время, имеют

закрытую архитектуру, что делает невозможным доступ пользователя к внутренним массивам данных этих систем.

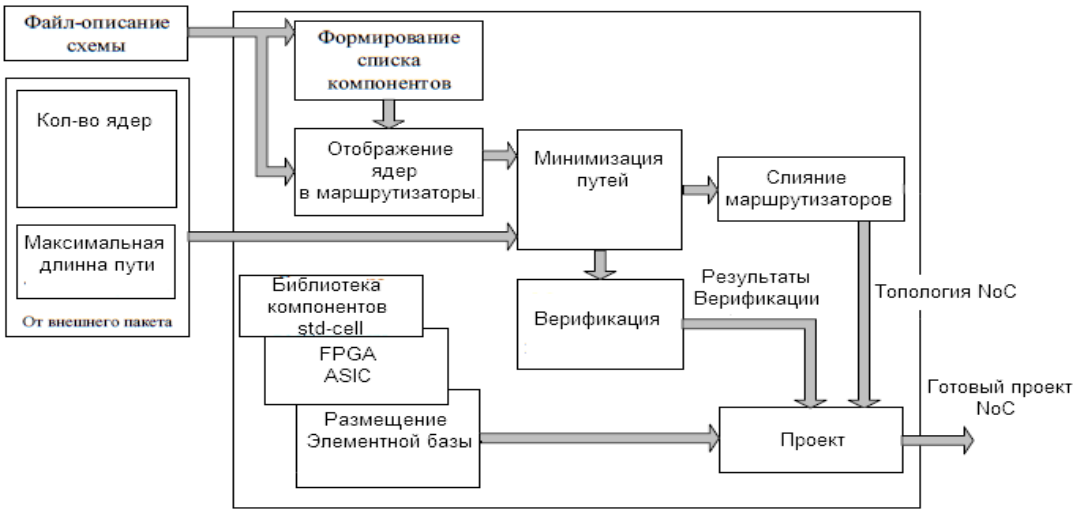



Рис.3.1.2

Базовая программа, является основной в иерархии программных модулей комплекса. Она реализует пользовательский интерфейс в защищаемой сети, а также управление работой комплекса, она позволяет управлять следующими функциями:

- работа с проектом;
- генерация топологии защищаемой сети;
- поиск неисправности или несанкционированного проникновения в сеть[99];
-экспорт в САПР.

## 3.2. Математические модели нечеткой базы знаний и алгоритма интеллектуальной системы поддержки принятия решений в задачах по защите информации в КС.

Нами разработана [23, 27, 99, 101, 104] 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,

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

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

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

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 [20].

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:**

$$\boldsymbol{R} = \left\| \boldsymbol{r_{ij}} \right\|, \tag{3.2.1}$$

где

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

Обозначим $\boldsymbol{W}$ матрицу значений атрибутов по объектам базы знаний:

$$W = \left(\omega_{ij}\right), \tag{3.2.2}$$

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

**Кластеризация** - это объединение объектов в группы (кластеры) на основе схожести признаков для объектов одной группы и отличий между группами. Большинство алгоритмов кластеризации не опираются на традиционные для статистических методов допущения; они могут

использоваться в условиях почти полного отсутствия информации о законах распределения данных. Кластеризацию проводят для объектов с количественными (числовыми), качественными или смешанными признаками [51].

Для проведения процесса кластеризации базы знаний по некоторому $o_i$-му объекту кластеризатору необходимо найти $N-1$ векторов пересечения этого объекта с другими объектами $o_l$ базы знаний по $a_j$-м атрибутам:

1- Определить матрицу активности

$$\vec{\delta}_i = (\delta_{ilj})$$

$$\delta_{ilj} = \min(r_{ij}, r_{lj}), \qquad (3.2.3)$$

2- Обозначив $B_i$ подмножество пересечений $o_i$-го объекта с $o_l$-м объектом базы знаний, получим:

$$B_{il} = A_i \cap A_l = \{b_{ilj}\}, \qquad (3.2.4)$$

Где $\{b_{ilj}\}$-множество пресечение объекта $o_i$ с объектами $o_l$ по $a_j$-м атрибутамя;

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

$j = \overline{1,Q}$, $Q = n_i + n_l$ - множество всех атрибутов объектов $o_i$ и $o_l$ в базе знаний;

3- Можно построить нечеткое подмножество $\tilde{B}_{il}$, содержащее нечеткие степени соответствия $o_i$-го объекта с $o_l$-м объектом по $a_j$-м атрибутам:

$$\tilde{B}_{il} = (\tilde{b}_{ilj}), \qquad (3.2.5)$$

где

$$\tilde{b}_{ilj} = \frac{\delta_{ilj}}{1+\sigma_{ilj}}, \qquad (3.2.6)$$

$$\sigma_{ilj} = \sqrt{(\omega_{ij} - \omega_{lj})^2}. \qquad (3.2.7)$$

Где

$\sigma_{ilj}$ - мера различия;

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

$\omega_{lj} \in W_i$ - значения $a_j$-го атрибута по множеству значений объекта $\boldsymbol{o_l}$-м.

Мощности подмножества пересечения $\boldsymbol{o_i}$ с $\boldsymbol{o_1}$-м объектом находим по формуле:

$$C_{il} = |B_{il}|. \tag{3.2.8}$$

Расстояние между объектами $\boldsymbol{o_i}$ и $\boldsymbol{o_l}$ можно представить в виде

$$d_{il} = (n_i + n_l) - 2.C_{il}, \tag{3.2.9}$$

где

$\boldsymbol{n_i}$=| $A_i$| ; $\boldsymbol{n_l}$=| $A_l$| - мощности объектов $\boldsymbol{o_i}$ и $\boldsymbol{o_l}$ соответственно.

Степень соответствия $\boldsymbol{o_i}$ с $\boldsymbol{o_l}$ на уровне атрибутов вычисляем как минимум между величиной, обратной расстоянию $\boldsymbol{d_{il}}$ , и коэффициентом покрытия $\boldsymbol{\gamma_{il}}$

$$\mu_{il}(d_{il}) = \min\left(\frac{1}{1+d_{il}};\quad \gamma_{il}\right), \tag{3.2.10}$$

Где

$\gamma_{il} = \frac{C_{il}}{n_i}$ - коэффициент покрытия; $\mu_{il}$, $\gamma_{il} \in [0;\ 1]$. Здесь $\boldsymbol{d_{il}}$ выражает значение симметричной разницы между объектами $\boldsymbol{o_i}$ и $\boldsymbol{o_l}$.

Нечеткое разбиение позволяет просто решить проблему объектов, расположенных на границе двух кластеров - им назначают степени принадлежностей равные 0.5. Недостаток нечеткого разбиения проявляется при работе с объектами, удаленными от центров всех кластеров. Удаленные объекты имеют мало общего с любым из кластеров, поэтому интуитивно хочется назначить для них малые степени принадлежности. Однако сумма их степеней принадлежностей такая же, как и для объектов, близких к центрам кластеров, т.е. равна единице. Для устранения этого недостатка можно использовать возможное разбиение, которое требует, только чтобы произвольный объект из базы знание принадлежал хотя бы одному кластеру.

Кластеризации множества ***O*** базируется на идее распределения степени соответствии атрибутов универсального множества согласно с их рангами.

Для кластеризации множества ***O*** в зависимости от величины симметричной разницы между объектами базы знаний используем степень соответствии $\mu_{il}$ . В зависимости от величины $\mu_{il}$ создаем ***N*** кластеров с ***m*** числом нечетких классов различных рангов, центр которых определяем по формуле:

$$\tilde{s}_r = 2.r.h, \qquad r = \overline{0,m}, \qquad m = 4,$$

где

h = 0,125 - шаг кластеризации,

$\tilde{s}_r$ - центр нечеткого класса *r*-го порядка,

*r* - порядковый номер качества нечеткого класса.

Таким образом, для каждого $\tilde{K}_i$-го ($i \in N$) кластера имеем пять классов, т.е. при $\tilde{s}_r = 0$ мы говорим о классе нулевого ранга; при $\tilde{s}_r = 0.25$ имеем нечеткий класс первого ранга и т.д., чем выше ранг нечеткого класса, тем выше степень соответствия $o_i$ с $o_l$ объектом на уровне атрибутов.

Области определения нечетких классов $\tilde{K}_i$-го нечеткого кластера представлены в табл. 3.2.1.

Таблица. 3.2.1

| Порядковый номер класса (ранга класса) | Центр класса $\tilde{s}_r = 2.r.h$, h = 0,125 | Область определения класса |
|---|---|---|
| 0 | 0 | ≈ [0; 0,25] |
| 1 | 0,25 | ≈[0; 0,5] |
| 2 | 0,5 | ≈[0,25; 0,75] |
| 3 | 0,75 | ≈[0,5; 1] |
| 4 | 1 | ≈[0,75; 1] |

Из табл. 3.2.1 видно, что

$$\tilde{K}_i = \begin{pmatrix} \tilde{k}_{i0} \\ \tilde{k}_{i1} \\ \dots \\ \dots \\ \tilde{k}_{ir} \\ \tilde{k}_{im} \end{pmatrix} \text{ - нечеткий кластер,}$$

где

$\tilde{k}_{ir} = \left\{ \lambda(r, \mu_{il}) \middle/ (o_i, o_l) \right\}$ - нечеткий класс *r*-го ранга $\tilde{K}_i$-го кластера,

$$\lambda(r, \mu_{il}) = \max\left( 0; 1 - \frac{\sqrt{(2.r.h - \mu_{il})^2}}{2.h} \right) \qquad (3.2.11)$$

Соотношение (3.2.11) определяет *функцию принадлежности* $\boldsymbol{o_l}$-го объекта к нечеткому классу $\tilde{k}_{ir}$ $\tilde{K}_i$-го нечеткого кластера, образованного на основе $\boldsymbol{o_i}$-го объекта ($o_i \in O$).

На рис. 3.2.3 показан график распределения возможностей по $\tilde{K}_i$-му кластеру.

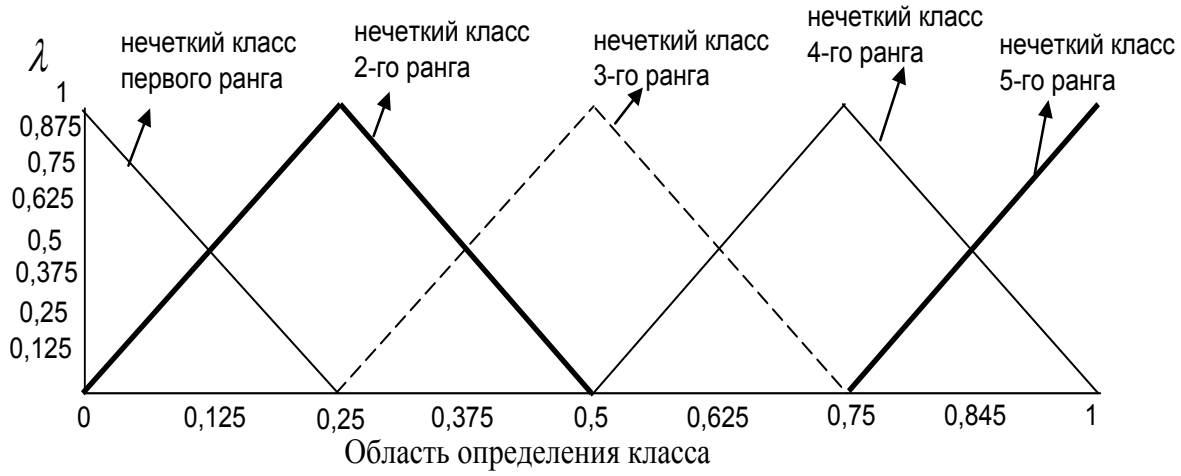



Рис. 3.2.3. Возможности

Вес $\boldsymbol{o_i}$-го объекта в $\tilde{k}_{ir}$ классе определяем по формуле

$$\theta_{ilr} = \lambda_{ilr} . \gamma_{il}\,, \qquad (3.2.12)$$

$$\theta_{ilr} \in [0;\ \ 1],$$

где $\gamma_{il}$ – коэффициент покрытия.

**Определение** [13].

Нечетким гипотетическим кластером уровня $\alpha \in [0;\ \ 1]$ называется нечеткое подмножество $\tilde{\mathrm{H}}_{\alpha} \subseteq \tilde{K}_i$, степень включения в $\tilde{K}_i$ которого определяем следующим образом:

$$\tau_{ilr}(\alpha) = \max[0; \theta_{ilr} - \min(1-\theta_{ilr}, \alpha)]. \qquad (3.2.13)$$

Значение $\alpha$ задается экспертом. По умолчанию $\alpha$ = 0,5. Элементами $\tilde{H}_{\alpha}$ являются те объекты $o_l \in \tilde{K}_i$, весовой коэффициент которых $\theta_{ilr}$ в $\tilde{k}_{ir} \subseteq \tilde{K}_i$ больше или равен $\alpha$:

$$\tilde{H}_{i\alpha} \left\{ \tau_{il\,r}(\alpha) \Big/ o_l \right\}, \qquad (3.2.14)$$

Обозначим $T\alpha$ - матрицу функции принадлежности $\boldsymbol{o_l}$-го $\tilde{H}_{i\alpha} \subseteq \tilde{K}_i$.

$$\mathrm{T}_{i\alpha} = \begin{pmatrix} 1 & \tau_{12} & \tau_{13} & \ldots & \tau_{1l} & \ldots & \tau_{1N} \\ \tau_{21} & 1 & \tau_{23} & \ldots & \tau_{2l} & \ldots & \tau_{2N} \\ \tau_{31} & \tau_{32} & 1 & \ldots & \tau_{3l} & \ldots & \tau_{3N} \\ \ldots & \ldots & \ldots & 1 & \ldots & \ldots & \ldots \\ \tau_{l1} & \ldots & \ldots & \ldots & 1 & \ldots & \tau_{lN} \\ \ldots & \ldots & \ldots & \ldots & \ldots & 1 & \ldots \\ \tau_{N1} & \tau_{N2} & \tau_{N3} & \ldots & \ldots & \ldots & 1 \end{pmatrix}. \qquad (3.2.15)$$

Как видно, по диагонали матрицы $T_{i\alpha}$ стоят $\tau_{11} = \tau_{22} = \tau_{il} = \tau_{NN} = 1$, это означает, что любой объект базы знаний на 100 % идентичен самому себе.

База знаний структурируется по *уровням* в зависимости от мощностей объектов.

Принадлежность объекта к тому или иному *уровню базы знаний* определяется следующей функцией:

$$g_k = \max\left(0; 1 - \sqrt{(n_i - k)^2}\right), \qquad (3.2.16)$$

где

$k = \overline{1, Z}, \quad Z = \sup\pi, \quad \pi = \{n_i\}, \quad n_i = |A_i|, \quad A_i \subseteq A$ .

Функция (3.2.16) принимает значения **1**, когда $\boldsymbol{n_i}$ равно $\boldsymbol{k}$, и **0** в противном случае, т.е.

$$g_k = \begin{cases} 1, & \textit{если} \quad \mathrm{n_i} = k \\ & \\ 0, & \textit{если} \quad \mathrm{n_i} \neq k \end{cases}. \qquad (3.2.17)$$

Все объекты с одинаковой мощностью находятся в одном уровне базы знаний. Чем больше значения мощности, тем выше уровень объекта в структуре уровней базы знаний.

**Определение** [16].

Мощность объекта - количество атрибутов, входящих в этот объект. Чем большим количеством атрибутов располагает объект, тем большее количество объектов из базы знаний с меньшим количеством атрибутов он покрывает.

Кластеризация объектов по классам кластеров с разным рангом и иерархическая структуризация базы знаний по уровням позволяют эффективно строить логическую цепочку в процессе вывода знаний для идентификации неизвестного объекта $X \notin O$. Кроме того, такой подход к организации базы знаний дает возможность получить ответы на вопросы, что общего (различного) имеется между кластерами объектов. Это, в свою очередь, способствует правильности концептуального анализа знаний.

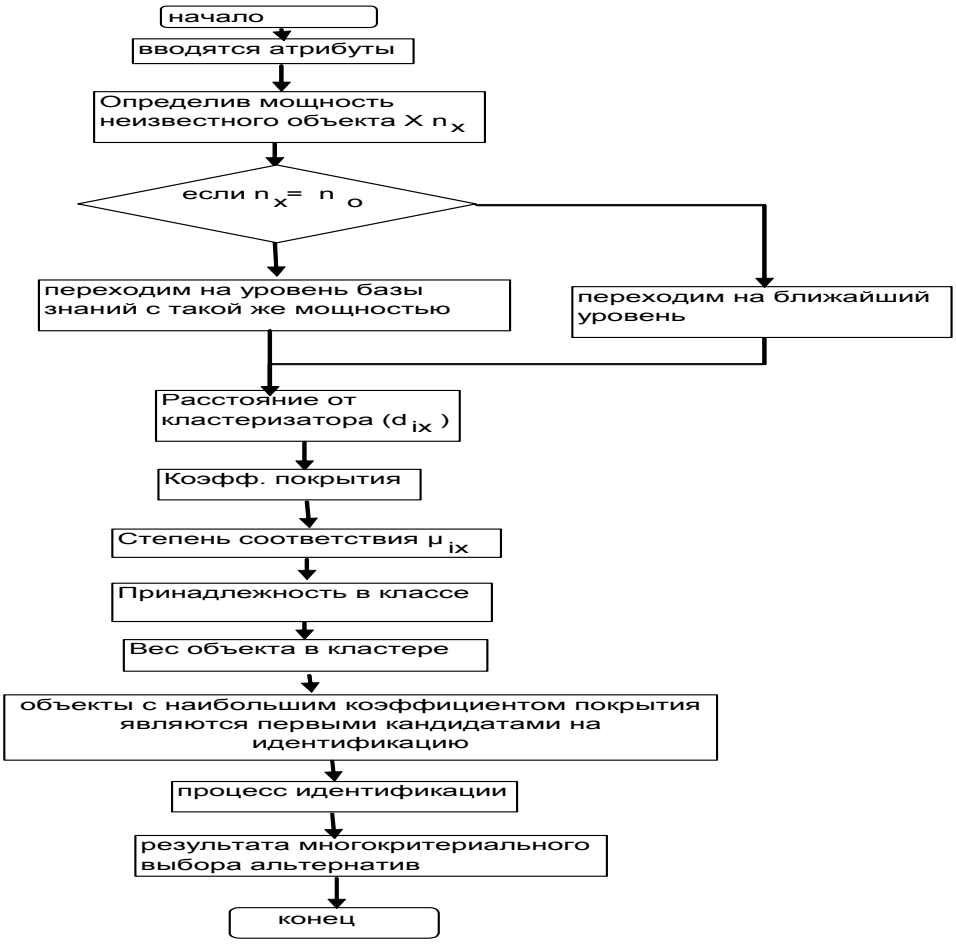


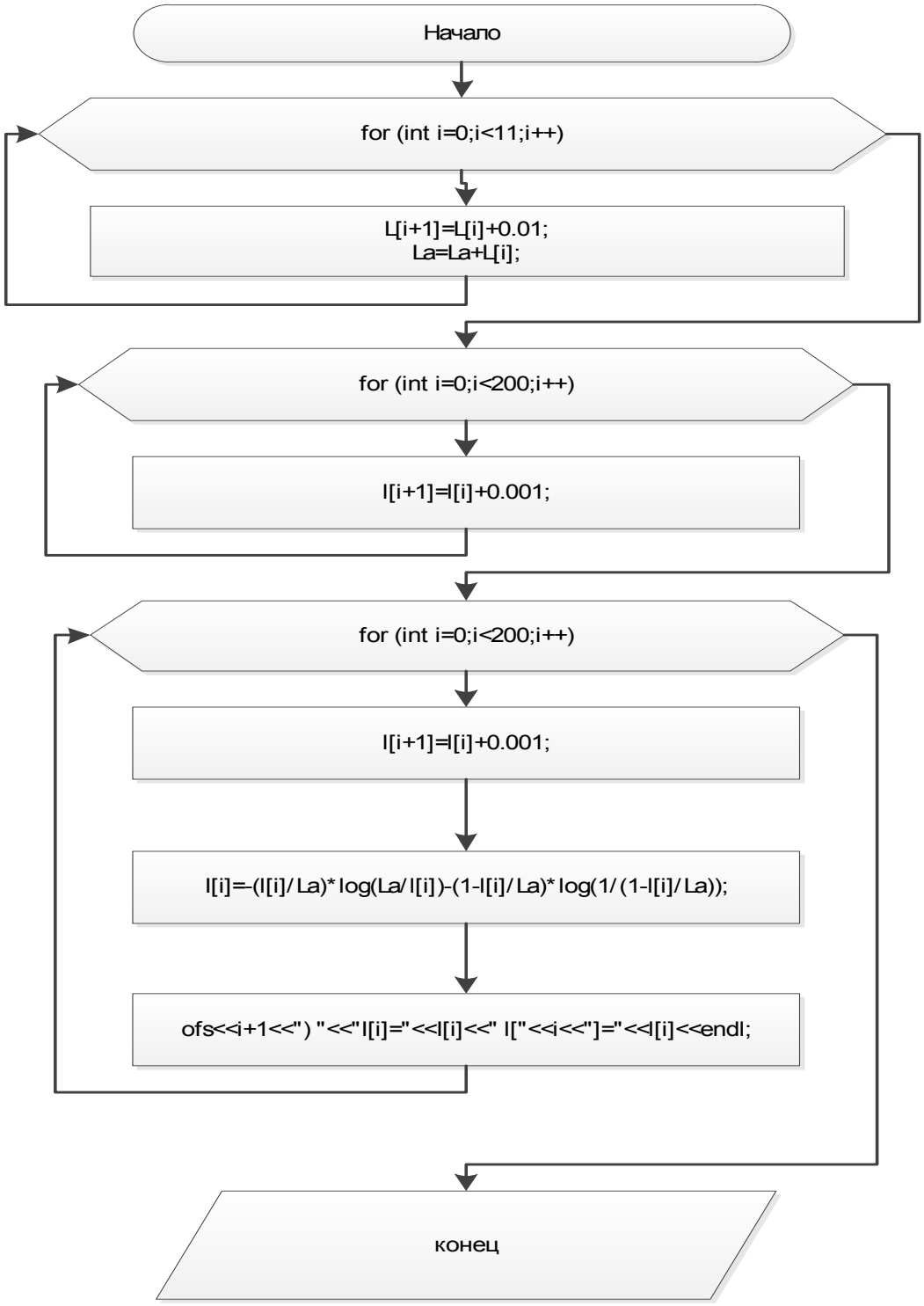

Рис.3.2.4. Структура алгоритма ИСППР для защиты информации

Вывод и идентификация неизвестного объекта $X \notin O$ на основе имеющихся знаний в базе знаний осуществляются следующим образом.

Сначала вводятся атрибуты и определяется мощность неизвестного объекта X. Определив мощность неизвестного объекта $\mathbf{n_x}$, переходим на соответствующий уровень базы знаний с такой же мощностью, если он есть, в противном случае переходим на ближайший уровень. Установив ближайший по значению мощности уровень базы знаний, проводим по соотношениям (3.2.1), (3.2.3), (3.2.8-16) процесс классификации в пространстве атрибутов для всех объектов этого уровня. Объекты, находящиеся в высшем классе гипотетического кластера $\tilde{H}_{x\alpha}$, образованного на основе объекта **X** на текущем уровне базы знаний, т.е. объекты $o_i \in O$ с наибольшим коэффициентом покрытия объекта **X** на основе атрибутов на текущем уровне базы знаний, являются первыми кандидатами на

идентификацию (сопоставление, отождествление) на уровне значений атрибутов.

Для улучшения экспертных оценок в ИСППР нами разработан алгоритм и программа, которые реализуют приведенный нами подход, и получены с ее помощью числовые данные, которые мы используем для анализа устойчивости результатов и возможности их использования в инженерных расчетах при проектировании и эксплуатационной защиты КИТС. При этом экспертные оценки не только улучшаются, но и упрощаются.




1) I[i]=-0.000981296 l[0]=0.001
2) I[i]=-0.0018299 l[1]=0.002
3) I[i]=-0.00262841 l[2]=0.003
4) I[i]=-0.00339438 l[3]=0.004
5) I[i]=-0.00413626 l[4]=0.005
6) I[i]=-0.00485872 l[5]=0.006
7) I[i]=-0.00556525 l[6]=0.007
8) I[i]=-0.00625804 l[7]=0.008
9) I[i]=-0.0069388 l[8]=0.009
10) I[i]=-0.00760889 l[9]=0.01
11) I[i]=-0.00826936 l[10]=0.011
12) I[i]=-0.00892121 l[11]=0.012
13) I[i]=-0.00956505 l[12]=0.013
14) I[i]=-0.0102014 l[13]=0.014
15) I[i]=-0.0108309 l[14]=0.015
16) I[i]=-0.0114541 l[15]=0.016
17) I[i]=-0.0120714 l[16]=0.017

18) I[i]=-0.0126829 l[17]=0.018
19) I[i]=-0.0132891 l[18]=0.019
20) I[i]=-0.0138903 l[19]=0.02
21) I[i]=-0.0144866 l[20]=0.021
22) I[i]=-0.0150784 l[21]=0.022
23) I[i]=-0.0156659 l[22]=0.023
24) I[i]=-0.0162492 l[23]=0.024
25) I[i]=-0.0168285 l[24]=0.025
26) I[i]=-0.0174038 l[25]=0.026
27) I[i]=-0.0179756 l[26]=0.027
28) I[i]=-0.0185438 l[27]=0.028
29) I[i]=-0.0191085 l[28]=0.029
30) I[i]=-0.01967 l[29]=0.03
31) I[i]=-0.0202283 l[30]=0.031
32) I[i]=-0.0207835 l[31]=0.032
33) I[i]=-0.0213356 l[32]=0.033
34) I[i]=-0.0218848 l[33]=0.034
35) I[i]=-0.0224312 l[34]=0.035
36) I[i]=-0.0229749 l[35]=0.036
37) I[i]=-0.023516 l[36]=0.037
38) I[i]=-0.0240543 l[37]=0.038
39) I[i]=-0.0245902 l[38]=0.039
40) I[i]=-0.0251237 l[39]=0.04
41) I[i]=-0.0256547 l[40]=0.041
42) I[i]=-0.0261834 l[41]=0.042
43) I[i]=-0.0267097 l[42]=0.043
44) I[i]=-0.027234 l[43]=0.044
45) I[i]=-0.0277559 l[44]=0.045
46) I[i]=-0.0282757 l[45]=0.046
47) I[i]=-0.0287935 l[46]=0.047
48) I[i]=-0.0293092 l[47]=0.048
49) I[i]=-0.0298228 l[48]=0.049
50) I[i]=-0.0303346 l[49]=0.05

Полная выкладка расчетов приведена в приложении 3.2.1.

Из приведенных рисунков и таблиц и числовых параметров хорошо заметны устойчивость результатов, что приводит к оценке, удовлетворяющей по точностным характеристикам заказчиков (см. приложения).

## 3.3. Разработка методик идентификации и структур для управления безопасностью КИТС

Рассмотрим алгоритм поиска и построения структур роутеров для обеспечения информационной защиты в сетях.

Сначала построим матрицу уровней ***L***[98].

Уровнями будем называть ***x*** и ***y*** координаты, на которых лежат ядра.

В строках матрицы ***L*** будут лежать ***x***-ые уровни, соответственно в столбцах ***y***-ые уровни. Элементы матрицы, это ядра - лежащие на соответствующих уровнях.

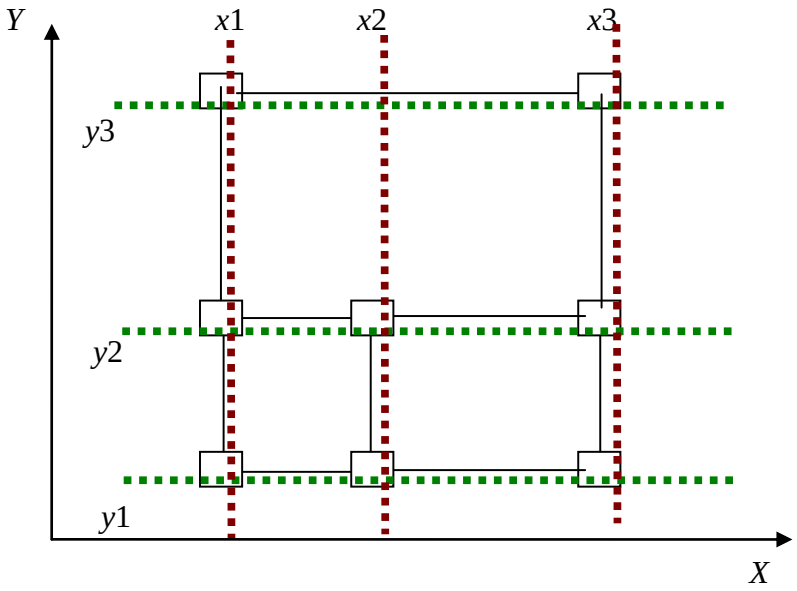



Рис 3.3.1. Соотношения и взаимодействия ядер

Чтобы построить матрицу *L* достаточно найти все уровни *x* или *y*. Их можно найти по следующему алгоритму:

Перебираем все ядра.

1.Возьмем *i*-е ядро

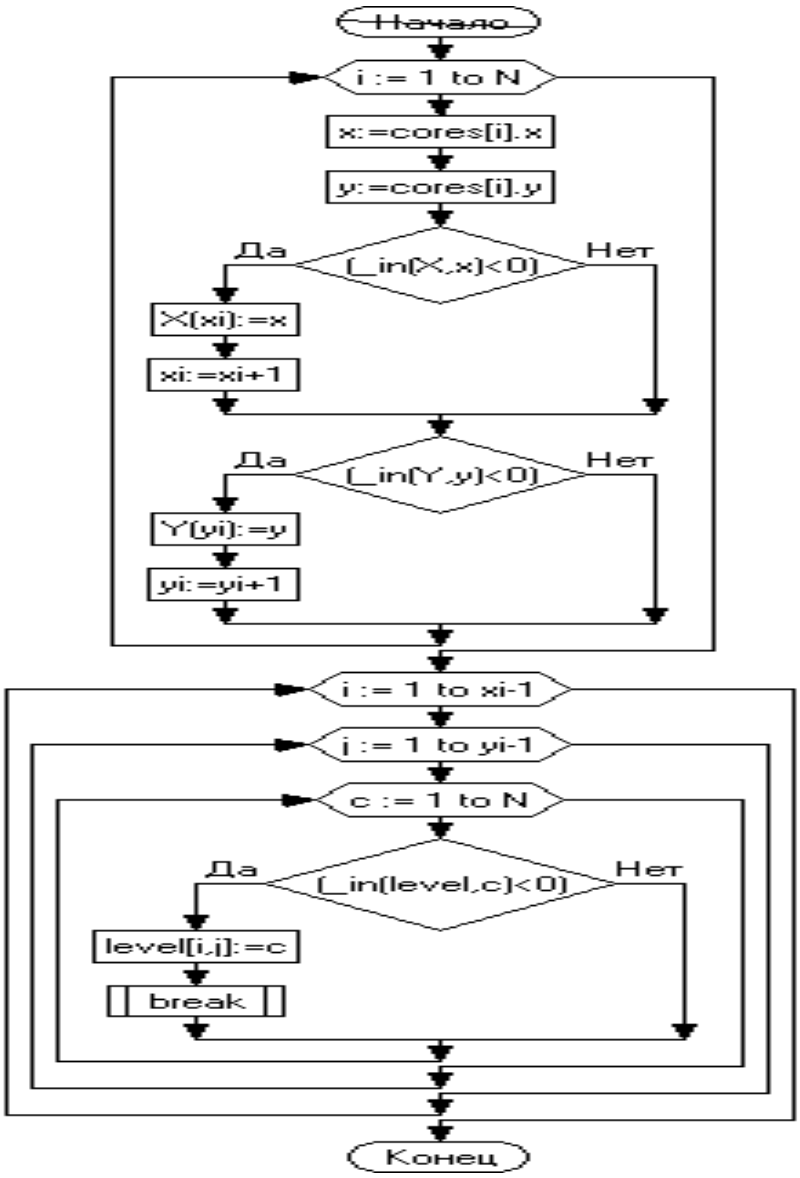
2.Проверяем, если оно не принадлежит ни одному из уровней, или уровни еще не созданы. Тогда создаем новый уровень, это будет новая строка в матрице *L*.

3.Далее для x-координаты находим все остальные ядра, лежащие на этом уровне. Те *x* координаты, которых равны (см. рис.3.3.1).

В итоге получим матрицу *L*. И количество уровней *x* – *X* (количество строк в матрице), и количество уровней *y* – *Y* (количество столбцов).

Блок схема алгоритма:

-




// stdafx.cpp: исходный файл, содержащий только стандартные включаемые модули

// aaaa.pch будет предкомпилированным заголовком

// stdafx.obj будет содержать предварительно откомпилированные сведения о типе

#include "stdafx.h"

// TODO: Установите ссылки на любые требующиеся дополнительные заголовки в файле STDAFX.H

// , а не в данном файле

// stdafx.h: включаемый файл для стандартных системных включаемых файлов

```
// или включаемых файлов для конкретного проекта, которые часто используются, но
// не часто изменяются
//
#pragma once
#include "targetver.h"
#include <stdio.h>
#include <tchar.h>
// TODO: Установите здесь ссылки на дополнительные заголовки, требующиеся для программы.
```

После построения матрицы уровней *L*, находим начало будущих роутеров.

Как уже говорилось выше, роутеры начинаем строить с левого нижнего угла. Поэтому, проверяем каждое ядро на наличие соседей справа и сверху. При этом соседи справа должны лежать на одном *y*-ом уровне с текущим ядром, а сосед сверху на одном *x*-ом уровне. Далее будем работать только с теми ядрами, у которых есть такие соседи, назовем их “угловыми ядрами”.

Следует отметить, что наличие соседей справа и сверху - необходимое, но не является достаточным условием существованием роутера.

Для нахождения “угловых ядер”, возьмем ядро из матрицы *L* с индексами (*i, j*) , где *i* – это индекс по уровню *x*, а *j* – по *y*. И проверим есть ли у него связь с *L(i* + 1, *j)* и *L(i, j* + 1), если есть то ядро *L(i,j)* и есть “угловая точка” a, соответственно *L(i* + 1, *j)* и *L(i, j* + 1) , *c* и *b* (см рис.3.3. 2). Теперь остается найти точку *d*.

Для этого начиная с *L(i* + 1, *j*) двигаемся вниз, до уровня *L(i, j* + 1) и если находим ядро *L(i* + l, *j* + *k*) связанное с *L(i,* j + 1), это и есть искомая точка *d*. Если на уровне *i* + 1 не нашли точку *d* , переходим к следующему уровню *i* + 2 и т.д. пока не будет найдена точка или же не закончатся ядра. Индексы *i,j* пробегают от 1 до *X* – 1 и от 1 до *Y* – 1, соответственно. Так как очевидно, что ядра находящиеся на последних уровнях не могут быть началами роутеров.

| | y1 | y2 | y3 |
|---|---|---|---|
| x1 | 1 | 4 | 7 |
| x2 | 2 | 5 | 0 |
| x3 | 3 | 6 | 8 |

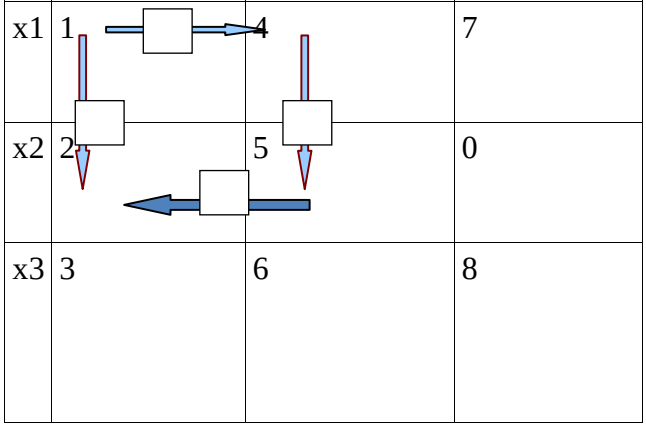


Рис.3.3.2. Номера на стрелках указывают порядок действий

Возьмем ядро 1. Оно находится на уровне *x*1 и *y*1.

Ищем его соседей с слева и сверху. Это ядра 4 и 2 если с ними есть связь, то это возможно роутер.

Далее начинаем двигаться от ядра 4, находящимся на уровне *x*1, *y*2 вниз до уровня на котором находится ядро 2 те *x*2. Там есть ядро 5, которое связано с 2 и 4, следовательно, роутер построен, и он состоит из ядер 1,2,4,5. По аналогии строим роутер 2,3,5,6 и 4,6,7.8.

После построения роутеров получаем массив роутеров *R*.

Каждый *R(i)* элемент которого, роутер и ядра, которые входят в него. Каждый роутер так же будет иметь начальные координаты *x*, *y* - это координаты левого нижнего угла, высоту *h* и ширину *w*.

По вышеприведенному алгоритму строятся все возможные роутеры. Минимизация ресурсов роутера приводит к сокращению статического расхода энергии и облегчению проектирования и верификации.

Очень часто цель состоит в том, чтобы минимизировать расход энергии[98,99] который выражается как

$$\text{Minimize } Z = \sum_{(i,k)\in E} \sum_{j\in R_i} \sum_{l\in R_k} \omega(i,k) \cdot \psi_l \cdot \text{dist}(j,l) \cdot X_{i,j,k,l} \tag{1}$$

где dist(*j*, *l*) является Манхэттанским расстоянием между этими двумя маршрутизаторами *j* и *l*. Проблема преобразования ядра в маршрутизатор эквивалентна проблеме max-flow min-cut и поэтому может быть оптимально решена в полиномиальное время.

Цепь минимизации может быть разделена на 2-е составляющих

$$Z = \sum_{(i,k),j,l} \sigma(i,k) \cdot x(j,l) \cdot X_{i,j,k,l} + \sum_{(i,k),j,l} \sigma(i,k) \cdot y(j,l) \cdot X_{i,j,k,l} \qquad (2)$$

где $\sigma(i, k) = \omega(i, k) \cdot \psi_l$, $x(j, l)$ является x-рассогласованием между двумя маршрутизаторами, и $y(j, l)$ является y-рассогласованием между двумя маршрутизаторами. Можно разделить проблему на две подпроблемы, которые определяют x- и y-координаты, соответственно, роутера, в который преобразовано ядро.

Можно уменьшить их количество путем объединения соседних роутеров.

При этом объединении нужно проводить таким образом, чтобы не пропадали ядра (см. пример на рис. 3.3.3). И длина пути не оказалась больше максимально разрешенной длины пути *D*

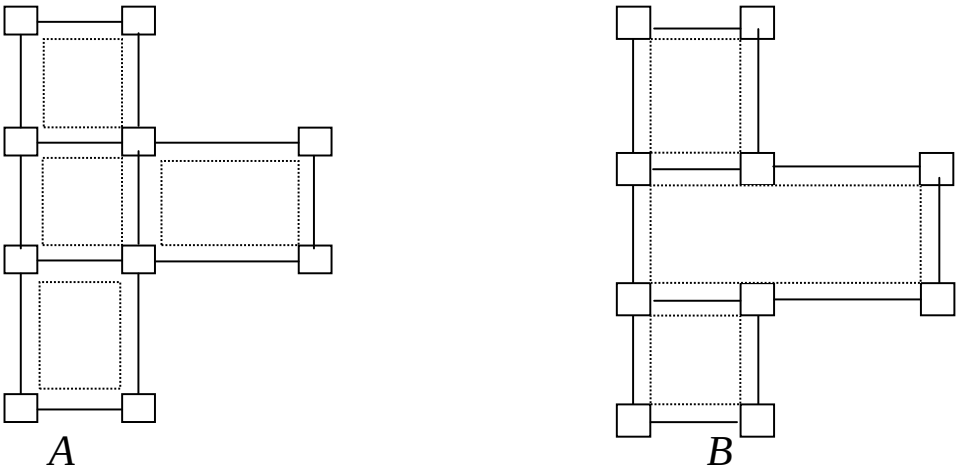
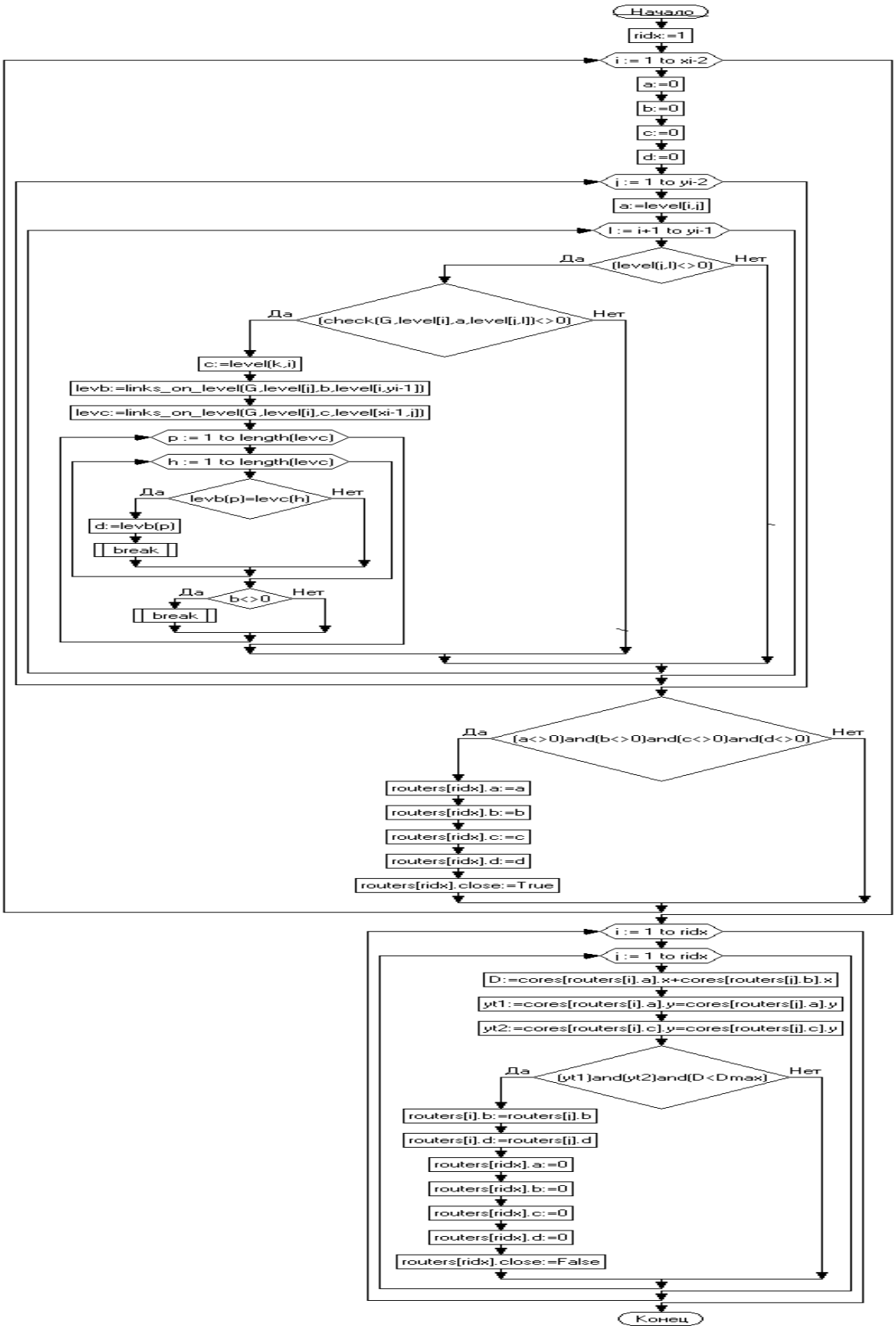



Рис 3.3.3. Объединение роутеров. *A* — до объединения, *B* — после.

На рис.3.3.3 изображены 10 ядер, связи между ними и 4 роутером.

Блок-схема алгоритма построения роутеров и уменьшения их количества:




```
#include "stdafx.h"
#include <stdio.h>
```

```
#include <iostream>
#include <string>
#include <cstdlib>
#include <math.h>
using namespace std;
int main()
{int a;
float l[202];
float I[202];
float L=0;
l[0]=0.001;
for (int i=0;i<200;i++)
{
l[i+1]=l[i]+0.001;
L=L+l[i];
//cout«L«endl;
}
cout«"L="«L«endl;
for (int i=0;i<200;i++)
{
l[i+1]=l[i]+0.001;
I[i]=-(l[i]/L)*log(L/l[i])-(1-l[i]/L)*log(1/(1-l[i]/L));
cout«i+1«") "«"I[i]="«I[i]«" l["«i«"]="«l[i]«endl;}
system ("pause");
return 0;}
```

Вспомогательные функции:

Функция *check* – проверяет - есть ли связь между двумя ядрами на уровне.

Функция *links_on_level* – возвращает массив ядер с которыми имеет связь текущее ядро.

Роутеры будем объединять следующим образом.

Возьмем R(i) роутер, и его соседей, если их ядра лежат на одинаковых x или y уровнях, тогда эти роутеры можно объединить в один. То есть один роутер является продолжением другого.

Например на рисунке 6. можно объединить роутеры 2 и 3, так как 3,4,5 и 6,7,8 образующие эти роутеры лежат на одинаковых y уровнях. При этом ядра 4,7 останутся в роутерах 4,1.

Но нельзя объединить роутеры 1,2,4 так как при этом произойдет исключение из топологии ядер 3 и 6.

Итак после объединения получаем минимизированное количество роутеров.

Нами было предложено[98, 99], что у каждого ядра есть только один порт ввода/вывода (*I/O*), который должен быть присоединен к единственному порту роутера. Можно тривиально допустить ядра с многочисленными портами ввода/вывода, которые должны быть преобразованы в определенные роутеры. По существу, каждый порт ядра должен быть смоделирован отдельным узлом в потоковом графе, чтобы решить этот вопрос[98-100].

В результате получаются топология с минимальными роутерами и самые короткие пути, Проиллюстрируем рис.3.3.4.

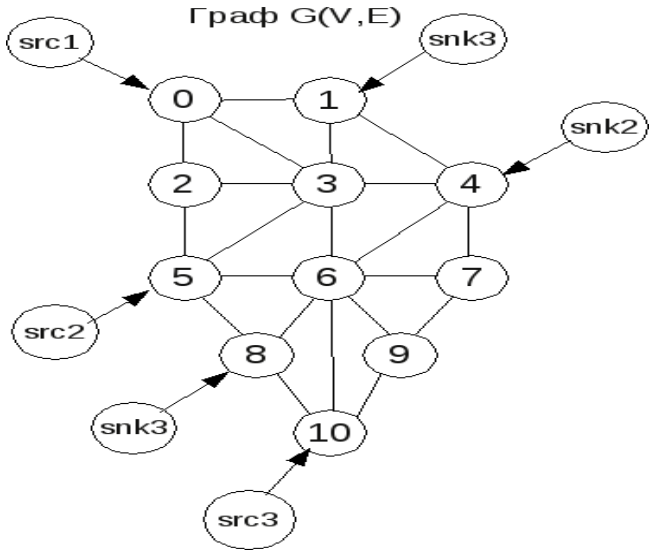



Рис.3.3.4-А.

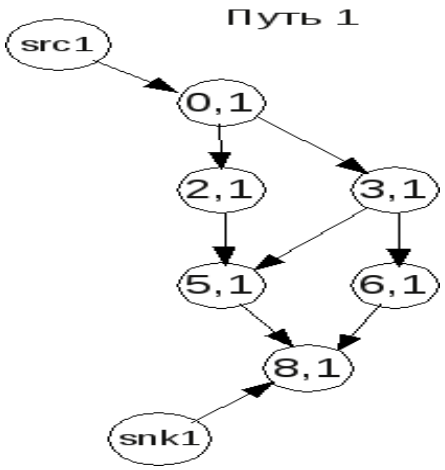



Рис.3.3.4.-Б

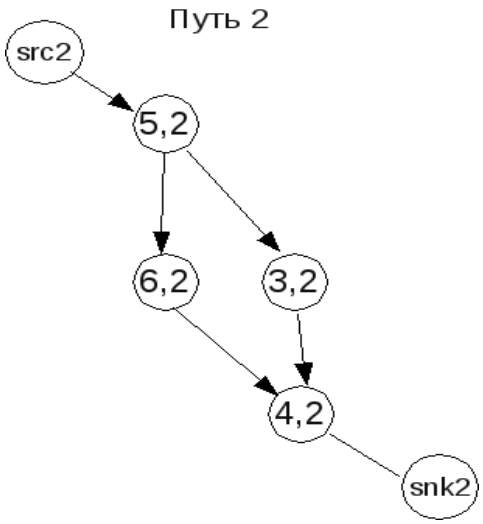



Рис.3.3.4.-В

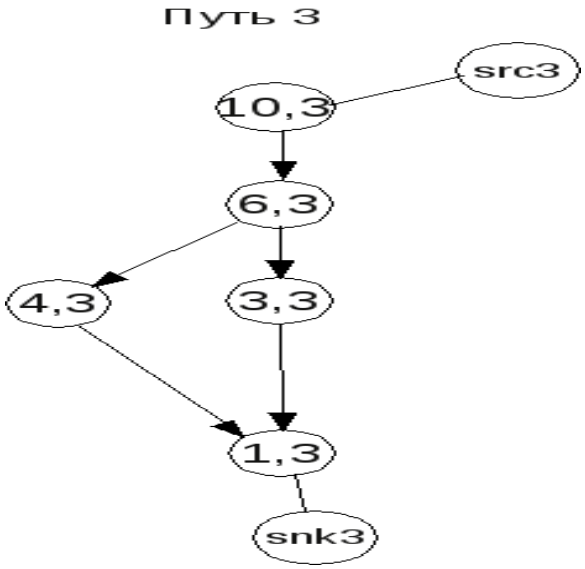



Рис. 3.3.4.-Г. Минимизация топологий роутеров.

Основанная на отсечении минимизация сформулирована как

$$\text{Minimize} \sum_{r} X_r$$

при условии

$$\forall C \sum_{\forall e((r,\text{tr}),(s,\text{tr}))\in\delta(C)} X_r \geq F(C).$$

Экспериментальное исследование предложенных моделей и алгоритмов осуществлялось с использованием специально разработанной программы.

Для демонстрации возможностей предложенной методики организации и извлечения знаний из базы знаний рассмотрено на расчете для сети завода

«Электроприбор» (г. Москва) (рис. 3.3.5, табл. 3.3.2).

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 корпоративных информационно-телекоммуникационных сетей)

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

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

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

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

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

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

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

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

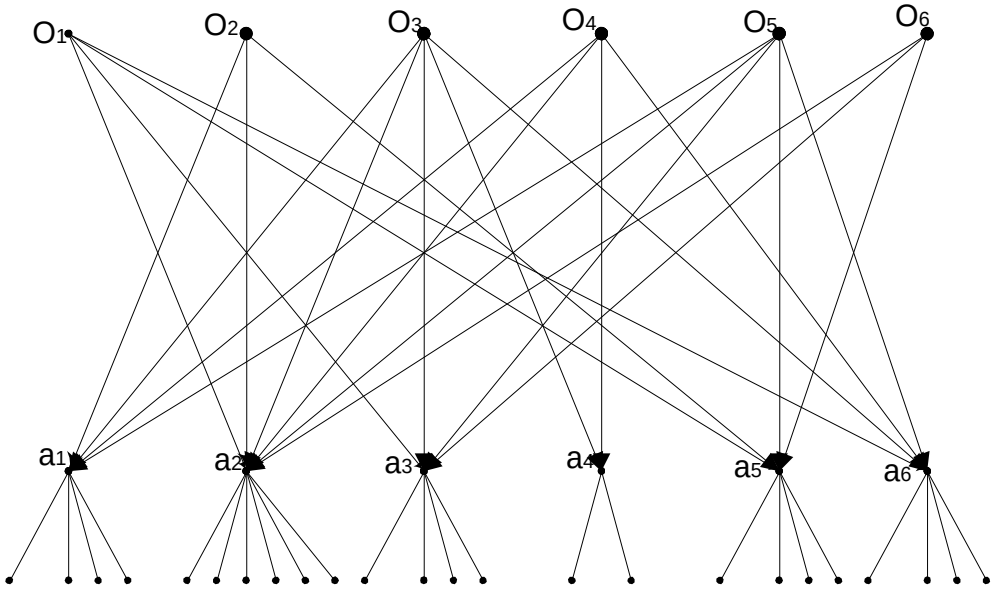
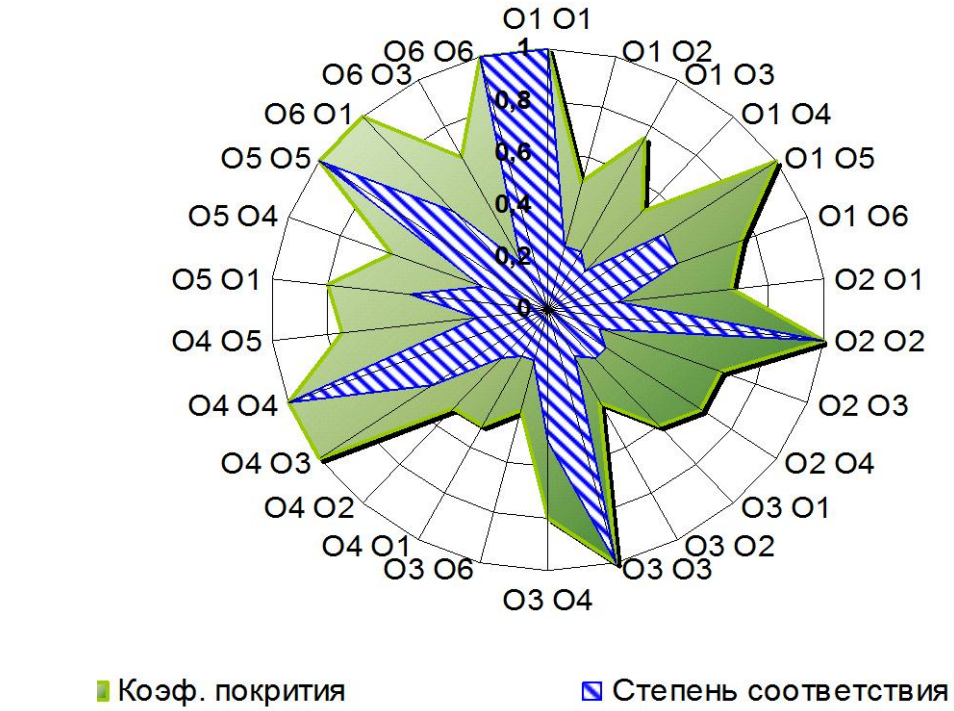
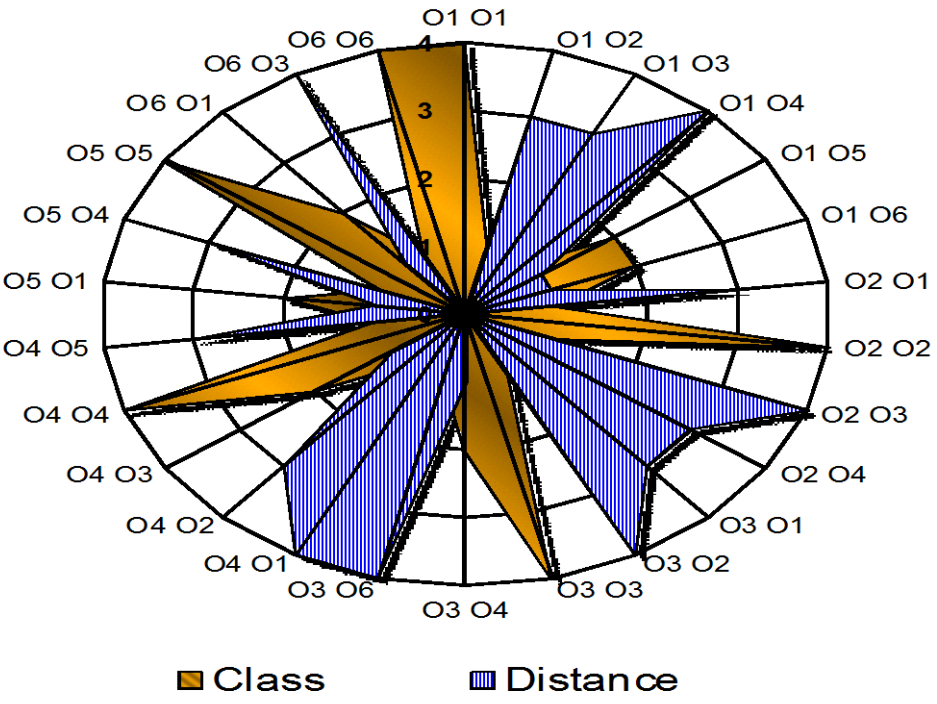



Рис. 3.3.5. Элементы нечеткой логики и объекты базы КИТС

На рис. 3.3.6 –11 показан предложенный нами подход нечеткого обобщения.

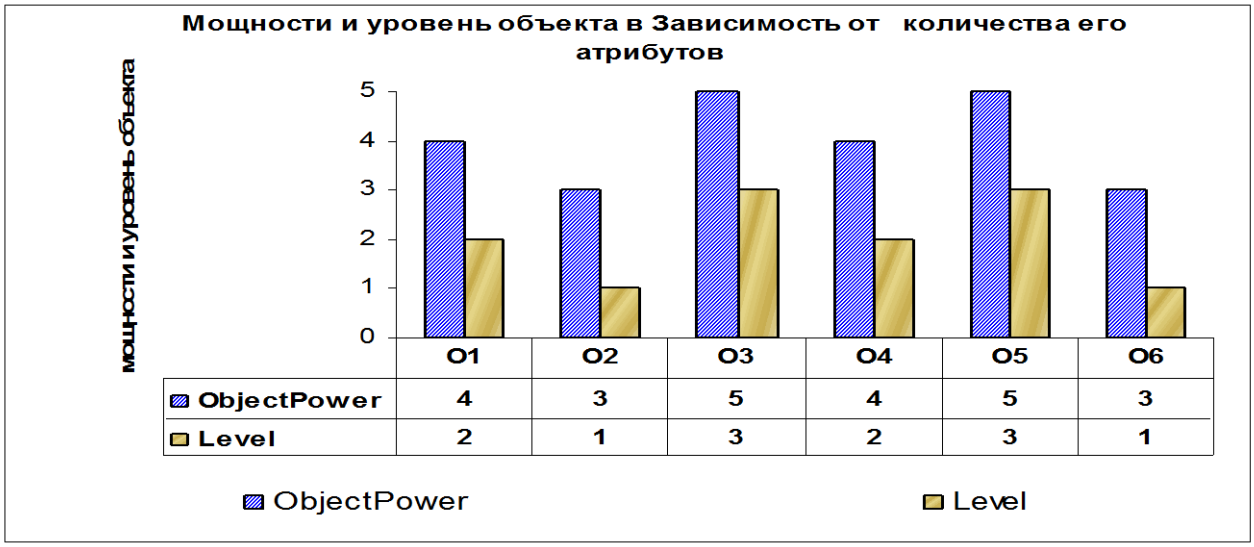


В табл. 3.3.3 структуризация знаний.

Таблица 3.3.3. Зависимости от мощностей

| Объект | Мощности объекта | Уровень объекта в БЗ |
|---|---|---|
| O1 | 4 | 2 |
| O2 | 3 | 1 |
| O3 | 5 | 3 |
| O4 | 4 | 2 |
| O5 | 5 | 3 |
| O6 | 3 | 1 |



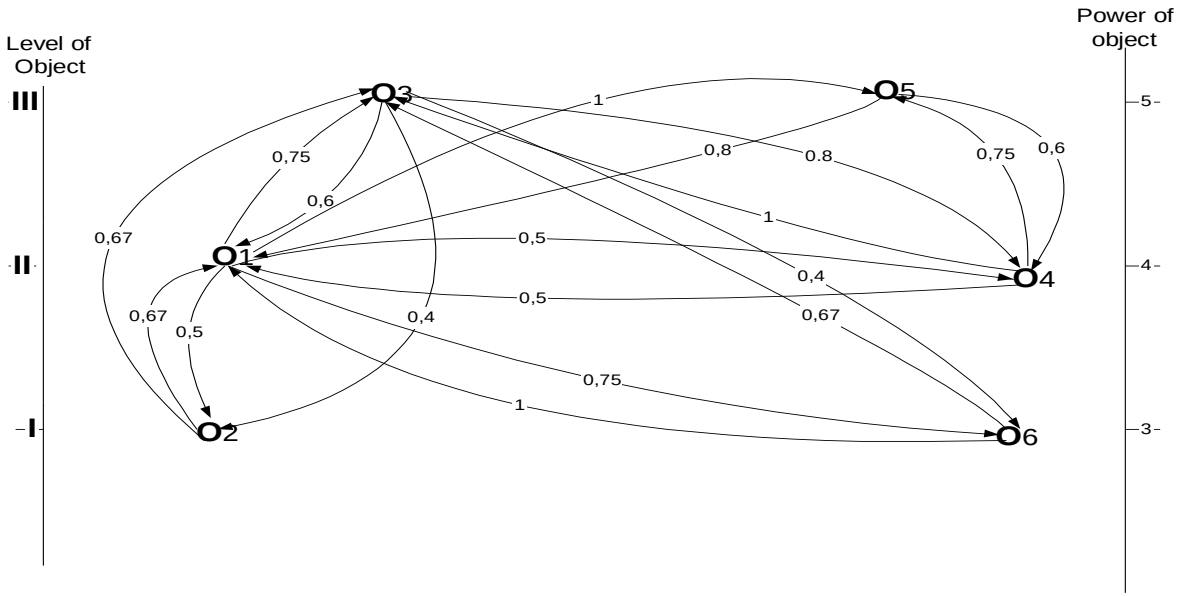




Рис. 3.3.9. График и структура базы знаний

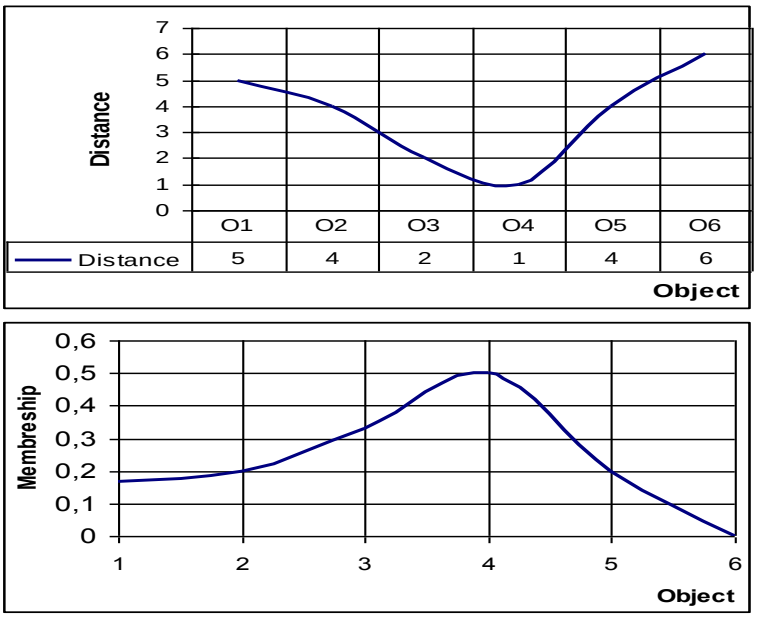



Рис.3.3.10.а) Влияние мощности объекта

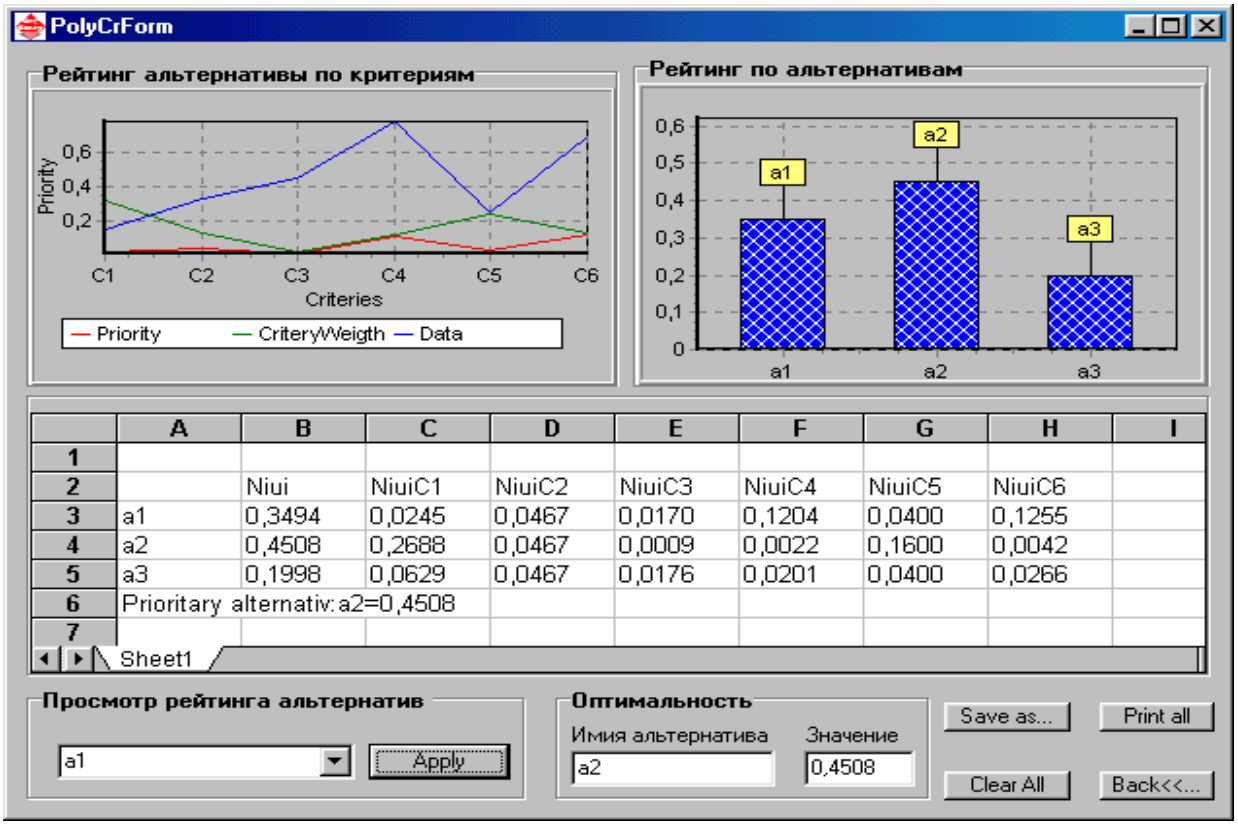



Рис. 3.3.11. Выбора альтернатив с учетом экспертных оценок

## 3.4. Повышение уровня информационной безопасности КИТС

Анализ рисков будем проводить в соответствии с разработанной нами методикой[23, 98-100]. Поскольку в настоящее время внедрение в Палестине проблематично, то используем для этого российские предприятия, аналогичные по сетевой структуре палестинским (использование телефонных модемов, маршрутизаторов, малые скорости и память).

Структурная схема сети одного из таких предприятий ООО «Электроприбор» (г. Москва) представлена на рис.3.4.1. КИТС имеет доменную структуру. Домен – группа компьютеров, образующих часть сети и использующих общую базу данных каталога. Каждый домен имеет уникальное имя. Таким образом, доменная архитектура представляет собой централизованный вариант управления сетью.

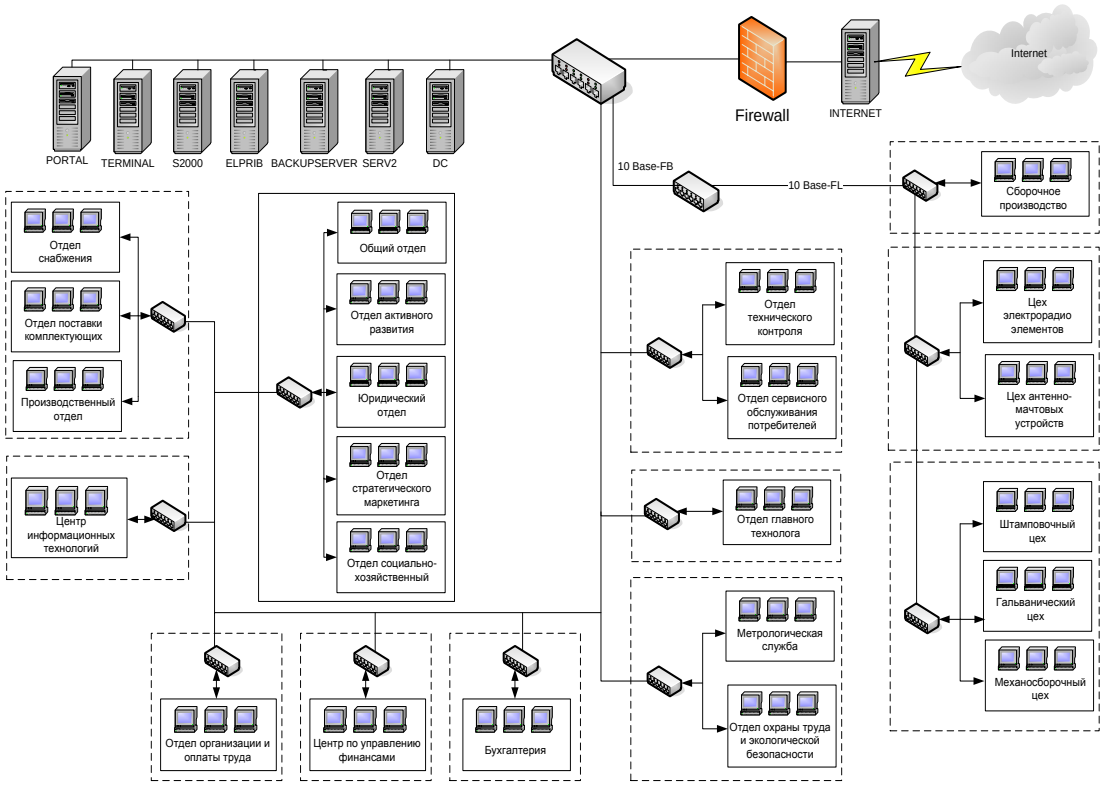



Рис. 3.4.1. – Упрощенная структура сети завода

Рассмотрим вопросы внедрения разработанных нами методик управления безопасностью на практике.

**Структура активов корпоративной сети.**

АРМЫ сотрудников предназначены для составления, хранения и обработки документов с грифом «Коммерческая тайна», «конфиденциально», а также неконфиденциальных документов. Доступ исполнителей к работе на ПЭВМ, осуществляется по утвержденному списку. Предполагается наличие только постоянных пользователей. Пользователи имеют право постоянного хранения файлов с конфиденциальными данными на ЖМД. Для хранения файлов с конфиденциальными данными могут также использоваться оптические носители, в установленном порядке. Загрузка всех АРМ осуществляется по персональным имени и паролю пользователя. По окончании загрузки компьютера пользователь получает установленные Администратором безопасности права доступа к устройствам, каталогам и файлам и программам ПЭВМ. Для разработки документов установлен программный пакет Microsoft Office. Права доступа пользователей к программам, каталогам и файлам на ПЭВМ определены в документации по разрешительной системе доступа персонала к защищаемым ресурсам ПЭВМ. Антивирусная защита осуществляется пользователями ПЭВМ с применением программного средства «Антивирус Касперского». Перезагрузка серверов происходит 1 раз в неделю, перерыв работоспособности не более 5 мин. Архивирование и резервное копирование данных системы и конфигураций оборудования производится каждый день.

**Размещение информационных ресурсов в корпоративной сети.**

В состав КИТС ООО «Электроприбор» (г.Москва) входят: контроллер домена, сервер для работы бухгалтерской программы «Инфин», дополнительный контроллер домена, сервер АСУ, сервер-терминал, сервер резервного копирования, интернет-сервер, внутренний web-сервер, АРМы пользователей.

Термин «общие активы информационной системы» относится как к физическим, так и логическим аспектам предприятия. Они могут включать в себя серверы, рабочие станции, программное обеспечение и пользовательские лицензии [52,60].

Данные о деловых контактах сотрудников, данные о сотрудниках, стратегические планы, внутренние web-узлы и пароли сотрудников являются общими активами информационной системы.

Список активов корпоративной вычислительной сети ООО «Электроприбор» (г. Москва) приведен в табл. 3.4.1.

| Класс актива | Описание актива | Описание следующего уровня |
|---|---|---|
| Материальный | Физическая инфраструктура | Серверы |
| Материальный | Физическая инфраструктура | Настольные компьютеры |
| Материальный | Физическая инфраструктура | Серверное программное обеспечение |
| Материальный | Физическая инфраструктура | Программное обеспечение для конечных пользователей |
| Материальный | Физическая инфраструктура | Средства разработки |
| Материальный | Физическая инфраструктура | Маршрутизаторы |
| Материальный | Данные интрасети | Данные о личных контактах сотрудников |
| Материальный | Данные интрасети | Данные о заказах |
| Материальный | Данные интрасети | Схема инфраструктуры сети |
| Материальный | Данные интрасети | Внутренние веб-узлы |
| Материальный | Данные экстрасети | Данные о контрактах с партнерами |
| Материальный | Данные экстрасети | Финансовые данные о партнерах |
| Материальный | Данные экстрасети | Данные о заказах партнеров |
| Материальный | Данные экстрасети | Отчеты о кредитах поставщиков |
| Материальный | Данные экстрасети | Данные о заказах поставщиков |
| Службы ИТ | Обмен сообщениями | Веб-клиент Microsoft Outlook® |
| Службы ИТ | Инфраструктура ядра | Система доменных имен (DNS) |
| Службы ИТ | Инфраструктура ядра | Корпоративные средства управления (АСУ) |

Идентификация существующих угроз безопасности и уязвимостей, делающих возможным осуществление угроз**.** На данном этапе составляется перечень угроз и оценивается их уровень, при этом могут быть использованы списки классов угроз различных организаций, а также информация о рейтингах либо средних значениях вероятности реализации данной угрозы. Подобные списки составляют и поддерживают в актуальном состоянии несколько организаций, в частности Federal Computer Incident Response Center (FedCIRC), Federal Bureau of Investigation's National Infrastructure Protection Center, SecurityFocus и др. [94].

В данном случае, данные об угрозах, характерных для корпоративной вычислительной сети ООО «Электроприбор» (г. Москва) предоставлены Администратором безопасности ЛВС предприятия и основываются на проведенных им исследованиях. Этот обширный список угроз и средств защиты, которым может быть подвержена корпоративные сети ООО «Электроприбор» (г. Москва), приведен в табл. 3.4.2.

Уязвимости представляют собой слабые места в процедурах и политиках безопасности КИТС, административном управлении, физическом размещении, внутреннем управлении и других областях, которые могут использоваться для получения несанкционированного доступа к сведениям или прерывания критически важных процессов. Уязвимости бывают как физическими, так и логическими. Табл.3.4.3-4.содержит список уязвимостей, которые могут проявляться в корпоративной сети предприятия, также предоставленный администратором безопасности ЛВС ООО «Электроприбор» (г. Москва).

Таблица 3.4.3

| № п\п | Наименование, источник | Возможные способы реализации | Действие, номера СЗ |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | Кража пароля или подбор пароля | Слежение за авторизованным пользователем. Получение пароля из файла, магнитного носителя, записной книжки, смарт-карты путем НСД, легального доступа или кражи. Полный перебор вариантов. | Компрометация пароля, возможность НСД к информации, доступной пользователю. 3, 6, 11 |
| 2 | Внедрение программ-закладок | Использование нелицензионного ПО. Запуск авторизованным пользователем неизвестных программ. Внедрение троянских программ из глобальных сетей | НСД к конфиденциальной информации, удаленное управление ВС. 9,8,6 |
| 3 | Заражение элементов вирусами | Использование нелицензионного ПО, файлов и носителей из ненадежных источников. Использование зараженных файлов из внешних сетей | Снижение качества обслуживания, нарушение конфиденциальности 9, 8, 6, 4 |
| 4 | Прослушивание информационного трафика | За счет особенностей сетевых протоколов, злоумышленник при подсоединении к сегменту ЛВС будет иметь доступ ко всему информационному обмену | Нарушение конфиденциальности информации. 1,2,5 |
| 5 | Сборка "мусора" (Вн. и внш..) | Злоумышленник считывает и анализирует удаленные файлы, файлы подкачки и т.п. | Нарушение конфиденциальности. 3,10 |

| | | | |
|---|---|---|---|
| 6 | Сканирование носителей информации | Злоумышленник последовательно пытается открыть файлы и папки с целью отыскать ошибки администрирования сети | Нарушение конфиденциальности. 6,7 |
| 7 | Запуск программы в качестве системной | Используя ошибки в ПО или администрировании ОС, злоумышленник получает полномочия, превышающие те, что были предоставлены ему. | Нарушение конфиденциальности, несанкционированная модификация. 6,8 |
| 8 | Подмена динамически загружаемой библиотеки | За счет получения привилегированного доступа к системным ресурсам злоумышленник внедряет в систем измененный вариант системной библиотеки | Нарушение конфиденциальности, несанкционированная модификация. 6,8 |
| 9 | Модификация кода или данных подсистемы защиты ОС. | За счет получения привилегированного доступа, злоумышленник имеет возможность изменить компоненты ОС с целью получения привилегированного доступа к данным | Нарушение конфиденциальности, несанкционированная модификация. 6,8 |
| 10 | Захват ресурсов. (Вн. и внш..) | Злоумышленник производит захват всех имеющихся в ОС ресурсов, программа входит в бесконечный цикл | Полный или частичных выход из строя ОС. 6,7 |
| 11 | Бомбардировка запросами. | Программа нарушителя постоянно направляет ОС | Снижение пропускной |

| | | | |
|---|---|---|---|
| | | запросы | способности каналов |
| 12 | Нарушение функционирования. | Отправление сообщения, которое временно или на длительный срок выводит из строя элемент системы | Вывод из строя системы или ее элементов. 5,6,7 |
| 13 | Использование ошибок в ПО или администрировании. | За счет ошибок в администрировании сети, сетевом программном обеспечении, злоумышленник получает доступ к конфиденциальной информации | Нарушение конфиденциальности информации, несанкционированное изменение информации. 5,6,7 |
| 14 | Навязывание сообщений. (Вн. и внш..) | Злоумышленник обманным путем переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей этих соединений | Навязывание ложной информации, внедрение вируса, нарушение процесса функционирования. 5,6,7 |
| 15 | Получение доступа к таблице маршрутизатора. | Получение информации с целью обеспечения возможности отправки ложных сообщений (маскарад) | Нарушение конфиденциальности информации. 1.5,6,7 |
| 16 | Изменение таблицы | Получение привилегированного доступа к маршрутизатору с | Нарушение конфиденциальн |

| | | | |
|---|---|---|---|
| | маршрутизатора. (Вн. и внш..) | целью изменения сетевых адресов его таблицы для перенаправления потока пакетов. | ости информации. 5,6,7 |
| 17 | Создание ложного маршрутизатора. | Злоумышленник создает ложный маршрутизатор и получает возможность перехватывать все сообщения, проходящие через него | Нарушение конфиденциальности информации. 1,5,6,7 |

Таблица 3.4.4

| № п/п | Класс уязвимости | Краткое описание уязвимости (пример) |
|---|---|---|
| 1 | Физический | Незапертые двери |
| 2 | Физический | Свободный доступ в помещения с компьютерами |
| 3 | Физический | Неэффективные противопожарные системы |
| 4 | Физический | Стены, подверженные физическому взлому |
| 5 | Оборудование | Исправления не установлены |
| 6 | Программное обеспечение | Устаревшее антивирусное программное обеспечение |
| 7 | Программное обеспечение | Исправления не установлены |
| 8 | Программное обеспечение | Небрежно написанные приложения (Использование межузловых сценариев) |
| 9 | Программное обеспечение | Сознательно созданные уязвимости («Черные ходы», оставленные производителями для управления или восстановления систем) |

| | | |
|---|---|---|
| 10 | Программное обеспечение | Сознательно созданные уязвимости (Программы-шпионы, например клавиатурные шпионы) |
| 11 | Программное обеспечение | Сознательно созданные уязвимости (Троянские программы) |
| 12 | Программное обеспечение | Сознательно созданные уязвимости |
| 13 | Программное обеспечение | Ошибки в конфигурации (Подготовка к работе вручную, приводящая к несогласованным конфигурациям) |
| 14 | Программное обеспечение | Ошибки в конфигурации (Системы не защищены) |
| 15 | Человеческий фактор | Плохо определенные процедуры (Плохой контроль над изменениями) |

**Механизмы (средства) защиты**. Перечень современных средств и методов защиты, способных с той или иной степенью эффективности блокировать выделенные угрозы приведен в табл. 3.4.5.

Таблица 3.4.5. Состав основных подходов к защите информации

| № | Наименование | Стоимо | Эффектив | Примечания |
|---|---|---|---|---|
| 1 | Средства шифрования | 2500 | Высокая | Тропа, VIPNet, |
| 2 | Средства шифрования отдельных сообщений | 250 | Высокая | Защищенная почтовая служба VIPNet, Курьер. |
| 3 | Средства криптографической | 250 | Высокая | Cryptomania, StrongDisk. |
| 4 | Средства организации электронной | 500 | Высокая | КриптоПро CSP, VCERT PKI |
| 5 | Межсетевые экраны | От 1500 до 40000 | Средняя | Застава-Джет, FortE+ (Застава-Элвис), FW-1, |

| | | | | |
|---|---|---|---|---|
| 6 | Средства аудита/протоколирования (анализа | 7505 (сегмент) 720 (на 1 | Средняя | RealSecure Network Sensor RealSecure OS Sensor |
| 7 | Сканеры безопасности | 1439 (на 10 устр.) 1001 (на 1 | Выше средней | Internet Scanner System Scanner Server Database |
| 8 | Средства контроля | 1000 | Высокая | |
| 9 | Антивирусные средства | 90 | Низкая | Dialogue Science DrWeb, AVP Kaspersky Labs, NAV for Windows, Symantec, VirusScan |
| 10 | Средства | 30 | Высокая | Программы-шреддеры |
| 11 | Средства | - | | Как правило |

Риски безопасности корпоративной сети.

Рекомендуемые контрмеры являются результатом процесса оценки рисков и, одновременно, входными данными для процесса нейтрализации рисков. Назначение рекомендуемых контрмер заключается в том, чтобы нейтрализовать (в достаточной степени уменьшить или устранить) идентифицированные риски. Нейтрализация рисков - вторая фаза процесса управления рисками — включает определение приоритетов, оценку и реализацию контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков.

Анализ воздействия - Предварительным условием проведения анализа воздействия является получение следующих сведений: процессы, выполняемые КИТС; критичность (ценность) подсистем и данных; чувствительность систем и данных. Воздействие, как и вероятность, можно оценить по трехбалльной шкале [24,93].

Поскольку полное устранение рисков невозможно и/или бессмысленно,

необходимо следовать принципу минимальной достаточности, реализуя только необходимые, наиболее подходящие механизмы безопасности с целью уменьшения рисков до приемлемого уровня с минимальными затратами [70].

В процессе управления рисками могут использоваться различные возможности [67-68] (табл.3.4.6):

Таблица 3.4.6. Управление рисками

| Действие | Устранение | Ответственность |
|---|---|---|
| принятие риска | На этапах: проекта, эксплуатации | заказчик |
| уклонение от риска | ликвидация причин и/или последствий риска, например, путем добавления механизмов безопасности, устранения небезопасных функций КИТС, приостановки работы КИТС в небезопасных ситуациях и т.п. | проект |
| ограничение риска | путем введения дополнительных средств защиты информации, уменьшающих воздействие угроз | Заказчик, проект |
| переадресация риска | путем приобретения страхового полиса | заказчик |

С практической точки зрения риски следует ранжировать, выделив наиболее опасные для КИТС. Основное правило управления рисками можно сформулировать следующим образом: начинать надо с наибольших рисков и стремитесь к их уменьшению до приемлемого уровня при минимальных затратах.

Если используются качественные методы, то возможные риски нарушения ИБ должны быть ранжированы по степени их опасности с учетом следующих факторов: цены возможных потерь, уровня угрозы и уязвимости.

Рассмотрим наиболее часто встречающийся вариант использования

качественных величин. Сначала необходимо определить шкалы. Субъективную шкалу вероятностей событий определим следующим образом табл.3.4.7):

Таблица 3.4.7. Субъективная шкала серьезности проишествий

| Событие, серьезность | Воздействия, |
|---|---|
| **A** | событие практически никогда не происходит |
| **B** | событие случается редко |
| **C** | вероятность события в данном промежутке около 50% |
| N (Negligible | происшествием можно пренебречь |
| Mi (Minor) | незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию незначительно |
| Mo (Moderate) | происшествие с умеренными последствиями: их ликвидация не связана с крупными затратами, воздействие на информационную технологию невелико и не затрагивает критически важные задачи |
| S (Serious) | происшествие с серьезными последствиями: их ликвидация связана с значительными затратами, воздействие на информационные технологии ощутимо и сказывается на выполнении критически важных задач |
| C (Critical) | C (Critical) - происшествие влечет за собой невозможность решения критически важных задач |

Для оценки рисков определяется субъективная шкала из трех значений: низкая степень риска; средняя степень риска; высокая степень риска.

В рассматриваемом варианте риск, связанный с конкретным событием, зависит от двух факторов и может быть определен так, как показано в табл3.4.8.

Таблица 3.4.8. Зависимость риска от угроз и ущерба

| | Negligible | Minor | Moderate | Serious | Critical |
|---|---|---|---|---|---|
| **A** | Низкий риск | Низкий риск | Низкий риск | Средний риск | Средний риск |
| **B** | Низкий риск | Низкий риск | Средний риск | Средний риск | Высокий риск |
| **C** | Низкий риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| **D** | Средний риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| **E** | Средний риск | Высокий риск | Высокий риск | Высокий риск | Высокий риск |

Рассмотрим на примере КИТС ООО «Электроприбор(г. Москва) повышение уровня информационной безопасности серверов. Значения (Критичность, Стоимость рисков) предоставлено администратором сети.

А. Рассматривается существующий вариант реализации защитных механизмов.

Исходные данные.

Имеется 8 серверов КТКС, по отношению, к которому рассматриваются семь уязвимостей (Таблица 2.2.7.) с вероятностями для каждого сервера: 0.1, 0.05, 0.2, 0.15, 0.18, 0.3 и 0.02. Первую уязвимость из них могут использовать две угрозы с вероятностями 0.35 и 0.65, вторую — три (0.4, 0.2, 0.4), третью — две (0.3, 0.7), четвертую — три (0.25, 0.25, 0.5), пятую — две (0.3, 0.7), шестую — (0.1,05,0.4), седьмую — (0.6,0.4).

Комплекс средств защиты, имеющийся в наличии содержит 3 средства защиты на каждый сервер (Экраны, Антивирусные, Пароля). Наконец, значения недостатков защитных механизмов оцениваются как 0.51, 0.6, 0.99.

Критичность серверов и их приблизительная стоимость приведены в табл. 3.4.9.

Таблица 3.4.9. Серверы и затраты на них

| № п/п | **Серверы КИТС** | **Критичность** | **Стоимость** |
|---|---|---|---|
| **1** | Контроллер домена - сервер | 0.9 | 3520 |
| **2** | Сервер для работы бухгалтерской программы «Инфин». | 0.8 | 1360 |
| **3** | Дополнительный контроллер домена | 0.7 | 1720 |
| **4** | Сервер АСУ. АСУ | 0.8 | 2964 |
| **5** | Сервер-терминал | 0.6 | 3524 |
| **6** | Сервер резервного копирования | 0.5 | 3544 |
| **7** | Внутренний web-сервер | 0.4 | 740 |
| **8** | Интернет-сервер | 0.6 | 884 |

Найти:

1. Величина риска?
2. Уровень риска?
3. Общий остаточный риск?
4. Ожидаемая сумма потерь и ожидаемая сумма затрат система?
5. Вероятность реализации злоумышленником всех целей?
6. Вероятность успешно комплекс средств защиты?

Решение задачи:

Множество выявленных уязвимостей серверов (так как конфигурации серверов, используемые аппаратно-программные средства, а также средства защиты, у всех одинаковые, то будем рассматривать для одного, но наиболее характерные), приведены в табл. 3.4.10.

Таблица 3.4.10. Уязвимости в сети в зависимости от классов

| № | **Класс уязвимости** | **Краткое описание уязвимости** | **Конкретный пример (если имеется)** | **Вероятность Уязвимости** |
|---|---|---|---|---|
| **1** | Программное обеспечение | Небрежно написанные приложения | Использование межузловых сценариев | 0.1 |
| **2** | Программное обеспечение | Сознательно созданные уязвимости | «Черные ходы», оставленные производителями для управления или восстановления систем | 0.05 |
| **3** | Программное обеспечение | Сознательно созданные уязвимости | Программы-шпионы, например клавиатурные шпионы | 0.2 |
| **4** | Программное обеспечение | Сознательно созданные уязвимости | Троянские программы | 0.15 |
| **5** | Программное обеспечение | Ошибки в конфигурации | Подготовка к работе вручную, приводящая к несогласованным конфигурациям | 0.18 |
| **6** | Программное обеспечение | Ошибки в конфигурации | Системы не защищены | 0.3 |

| | | | | |
|---|---|---|---|---|
| **7** | Человеческий фактор | Плохо определенные процедуры | Плохой контроль над изменениями | 0.02 |

2. Множество выявленных угроз, соответствующих данной всех цели приведены в табл.3.4.11.

Таблица 3.4.11.Возможные угрозы в КИТС при ИСППР

| **№** | **Наименование, источник** | $P_{уя}$ |
|---|---|---|
| **1** | Кража пароля или подбор пароля | 0.1 |
| **2** | Внедрение программ-закладок | |
| **3** | Заражение элементов вирусами | 0.05 |
| **4** | Прослушивание информационного трафика | |
| **5** | Сборка "мусора"(Вн. и внш..) | |
| **6** | Сканирование носителей информации | 0,2 |
| **7** | Запуск программы в качестве системной | |
| **8** | Подмена динамически загружаемой библиотеки | 0,15 |
| **9** | Модификация кода или данных подсистемы защиты ОС. | |
| **10** | Захват ресурсов. (Вн. и внш..) | |
| **11** | Бомбардировка запросами. | 0,18 |
| **12** | Нарушение функционирования. | |
| **13** | Использование ошибок в ПО или администрировании. | 0,3 |
| **14** | Навязывание сообщений. (Вн. и внш..) | |
| **15** | Получение доступа к таблице роутера. | |

| | | |
|---|---|---|
| **16** | Изменение таблицы роутера. (Вн. и внш..) | 0,02 |
| **17** | Создание ложного роутера. | |

3. Известные средства защиты, табл.3.4.12.

Таблица 3.4.12. Средства защиты

| № п/п | **Наименование** | **Стоимость** | **Эффективность** | **$P_{успех}$** | **недостатков** |
|---|---|---|---|---|---|
| **5** | Межсетевые экраны | От 1000 до 45000 | Средняя | 0.49 | 0.51 |
| **9** | Антивирусные средства | От 80 и выше | Низкая | 0.4 | 0.6 |
| **11** | Средства противодействия подбору пароля | - | - | 0.01 | 0.99 |

Таблица 3.4.13. Недостатки защиты

| **угрозы** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **5,9,11** | 11 | 9 | 9 | - | - | - | - | - | - | - | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| **недостатков защитных** | 0.99 | 0.6 | 0.6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0.51 | 0.51 | 0.51 | 0.51 | 0.51 | 0.51 | 0.51 |

Имеется M пар (активных угроз). Для каждой такой пары риск вычисляется по обычной формуле

$$R_k = P_i * I_j, \qquad (3.4.4)$$

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. Избыточные риски, которые требуется нейтрализовать, можно выразить соотношениями вида:

$$r_k = \begin{cases} R_k - R_a, & \text{если } R_k > R_a \\ 0, & \text{если } R_k <= R_a \end{cases} \qquad (3.4.5)$$

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

$$r_{Mean} = \frac{\sum_{k=1}^{N} r_k}{N} \qquad (3.4.6)$$

Значение $r_{Mean}$ можно рассматривать не только как средний избыточный риск, но и как оценку защищенности КИТС в целом. Эту оценку можно нормализовать, воспользовавшись формулой

$$r_{MeanNrorm} = \frac{r_{Mean}}{R_{\max} - R_a} \qquad (3.4.7)$$

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 отрезок [0, 1] можно разбить на интервалы, выделив тем самым нужное число уровней безопасности.

Кроме среднего арифметического, можно вычислить среднее квадратичное значение положительных избыточных рисков:

$$\sigma = \sqrt{\frac{\sum_{k=1}^{N} r_k^2}{N}} \qquad (3.4.8)$$

Как и средний избыточный риск, среднее квадратичное значение можно нормализовать:

$$\sigma_{Norm} = \frac{\sigma}{R_{\max} - R_a} \qquad (3.4.9)$$

Нормализованное среднеквадратичное значение, как и величину $r_{MeanNrorm}$, можно напрямую использовать для оценки уровня информационной безопасности КИТС, если разбить отрезок [0, 1] на соответствующее число интервалов. Значения, близкие к 0, свидетельствуют о высоком уровне защищенности, близкие к 1 —низком. Преимущество среднего квадратичного значения по сравнению со средним арифметическим в том, что первое более устойчиво к добавлению пар с небольшими избыточными рисками и более чувствительно к аномально высоким рискам.

Таблица 3.4.14. Зависимость риска от защиты

| $P_{уя}$ | 0.1 | | 0.05 | | | 0.2 | | 0.15 | | | 0.18 | | 0.3 | | | 0.02 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $P_{уг}$ | 0.35 | 0.65 | 0.4 | 0.2 | 0.4 | 0.3 | 0.7 | 0.25 | 0.25 | 0.5 | 0.3 | 0.7 | 0.1 | 0.5 | 0.4 | 0.6 | 0.4 |
| $P_{риск}$ | 0.035 | 0.065 | 0.02 | 0.01 | 0.02 | 0.06 | 0.14 | 0.0375 | 0.0375 | 0.125 | 0.054 | 0.126 | 0.03 | 0.15 | 0.12 | 0.012 | 0.008 |
| **Н** защ | 0.99 | 0.6 | 0.6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0.51 | 0.51 | 0.51 | 0.51 | 0.51 | 0.51 | 0.51 |
| Уровень риска | **Н** | **С** | **Н** | **Н** | **Н** | **С** | **С** | **Н** | **Н** | **С** | **С** | **С** | **Н** | **С** | **С** | **Н** | **Н** |

Можно воспользоваться еще одним представлением рисков — в виде деревьев уязвимостей, угроз и механизмов защиты [46,57,70], вид которого приведен на рис.3.4.2. Здесь $V_i$ — уязвимости, $T_{i,j}$ — угрозы, эксплуатирующие уязвимости, $C_{i,j}$ — средство защиты информации, нейтрализующее угрозу *i,j*, $L_{i,j}$ — недостаток защитных механизмов для угрозы *i,j*.

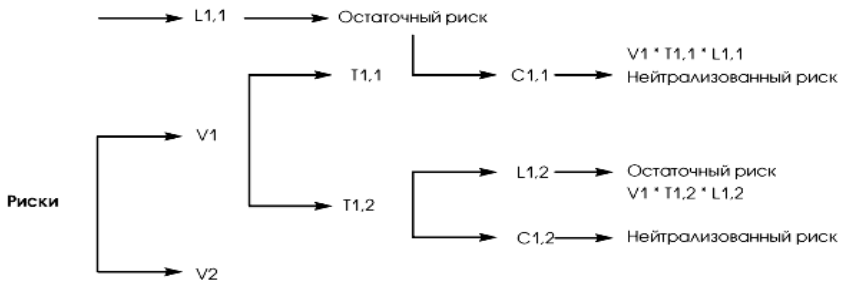



Рис.3.4.2. Уязвимости и угрозы

Значение для $V_i$, $T_{i.j}$, $L_{i.j}$ и $C_{i.j}$ предлагается нормировать, так чтобы

$$\sum_i (V_i + T_{i,j}) = 1, L_{i.j} + C_{i.j} = 1 \qquad (3.4.10)$$

Кроме вероятностных параметров, в оценке рисков участвуют константы — критичность активов ($C_A$) и их стоимость ($C_C$), Общий остаточный риск ($O_к$). Общая ожидаемая сумма потерь ($O_п$) выражается соотношением:

$$O_п = O_к * C_A * C_C$$

для нашей КИТС Общий остаточный риск составит: $O_{k1(5,9,11)} = 0.77065$

Ожидаемая сумма потерь: $O_{1п} = O_к * C_A * C_C$ (таблица 3.4.15).

Таблица 3.4.13. Потери от рисков

| № | Критичность | Стоимость$ | **$O_{k\,(5,9,11)}$** | | **Потерь$** | | **$O_{k\,(3,5,7,8)}$** | | **Потерь$** | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | K=1 | K=8 | K=1 | K=8 | K=1 | K=8 | K=1 | K=8 |
| **1** | 0.9 | 3520 | 0.771 | 1 | 2441.41 | 3168 | 0.2595 | 1 | 821.93 | 3168 |
| **2** | 0.8 | 1360 | | | 838.47 | 1088 | | | 282.3 | 1088 |
| **3** | 0.7 | 1720 | | | 927.87 | 1204 | | | 312.4 | 1204 |
| **4** | 0.8 | 2964 | | | 1827.4 | 2371.2 | | | 615.2 | 2371.2 |
| **5** | 0.6 | 3524 | | | 1629.5 | 2114.4 | | | 548.6 | 2114.4 |
| **6** | 0.5 | 3544 | | | 1365.6 | 1772 | | | 459.8 | 1772 |
| **7** | 0.4 | 740 | | | 228.11 | 296 | | | 76.8 | 296 |
| **8** | 0.6 | 884 | | | 408.8 | 530.4 | | | 137.61 | 530.4 |
| Сумма | | 18256 | | | 9667.16 | 12544 | | | 3254.64 | 12544 |

Вероятность реализации злоумышленником всех целей

$$P_{\text{уг,к1}}^{\text{зл}} = 3{,}201 * 10^{-3}$$

$$P_{\text{успешно}} = 1 - 3{,}201 * 10^{-3} = 0{,}998$$

Если повторная реализация угрозы ( $P_{aj}^{k} = P_{aj}^{k-1} + (1 - P_{aj}^{k-1})P_{e}$ ,

где к – число последовательно реализованных угроз $У_{Ге}$.).

Находим:

1- Вероятность реализации злоумышленником всех целей.

2- Вероятность успешного преодоления злоумышленником существующего комплекса средств защиты.

Результаты табл.3.4.16, рис.(3.4.3-5).

Результаты с комплексом средств защиты (Экраны, Антивирусные, Пароля).

Таблица 3.4.16. Потери и затраты

| **Повторная** | **Остаточный риск** | **Потерь** | **Затрат** | **Стоимость** | **Вероятность реализации злоумышленником** | **Вероятность успешно** |
|---|---|---|---|---|---|---|
| K=1 | 0,78065 | 770,65 | 3380,65 | 1610 | $3{,}2 * 10^{-3}$ | 0,998 |
| K=2 | 0,9533 | 953,3 | 35574,3 | 1610 | $6{,}39 * 10^{-3}$ | 0,995 |
| K=4 | 0,999 | 999,99 | 3499,9 | 1610 | $2{,}5 * 10^{-2}$ | 0,975 |
| K=6 | 0,999 | 999,99 | 3499,99 | 1610 | $9{,}74 * 10^{-2}$ | 0,903 |
| K=8 | 1 | 1000 | 3500 | 1610 | 3,36 *1 $0^{-1}$ | 0,664 |
| K=9 | 1 | 1000 | 3500 | 1610 | 6,71*1 $0^{-1}$ | 0,346 |
| K=10 | 1 | 1000 | 3500 | 1610 | 0,999 | 0,001 |

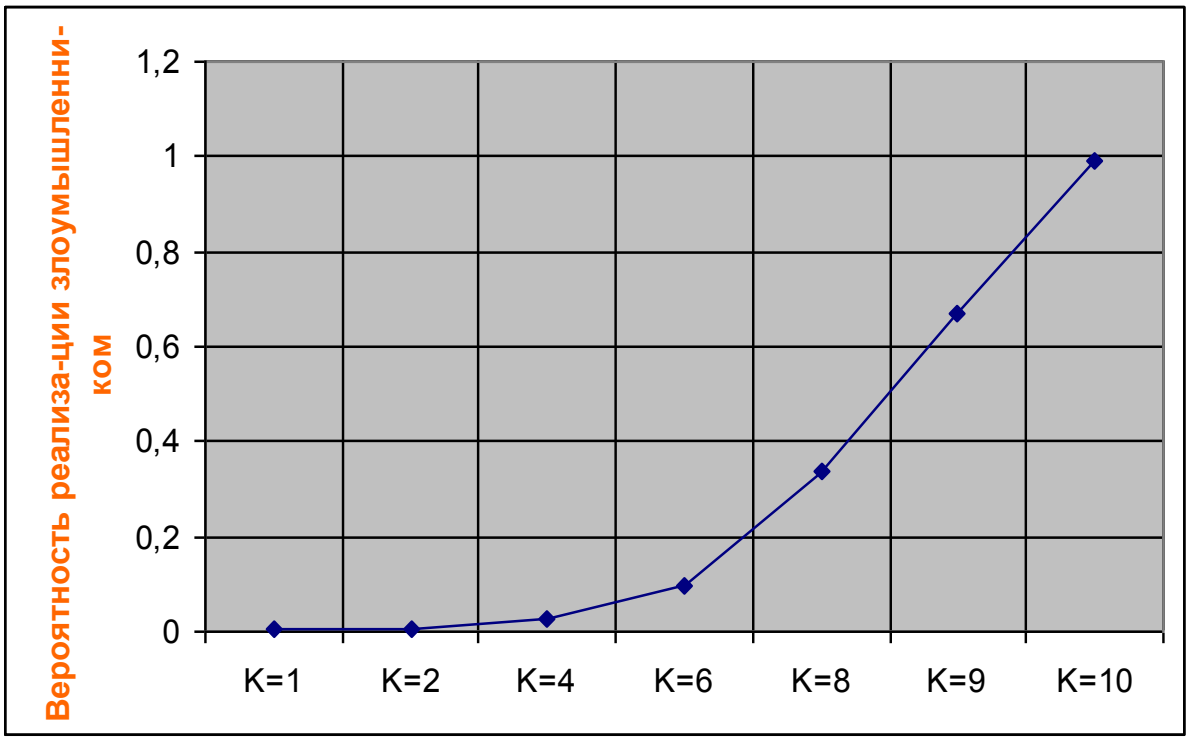



Рис 3.4.3. Достижения злоумышленником НСД от длительности

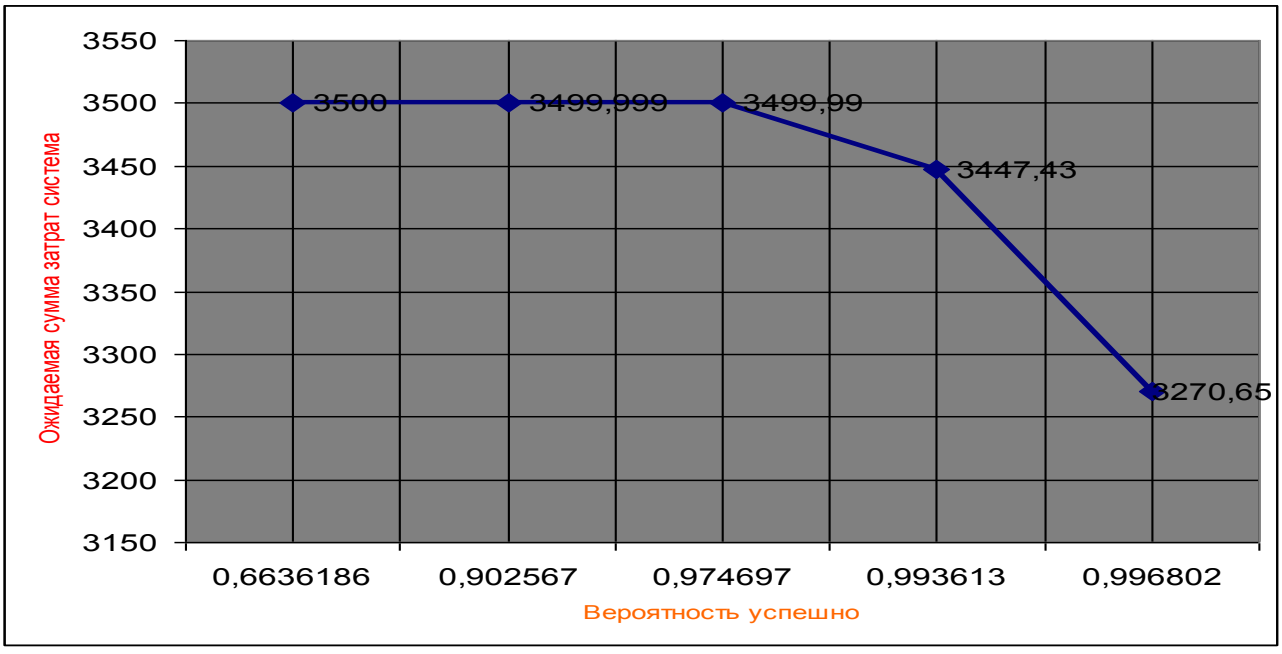



Рис 3.4.4. Затраты от успешного функционирования защиты

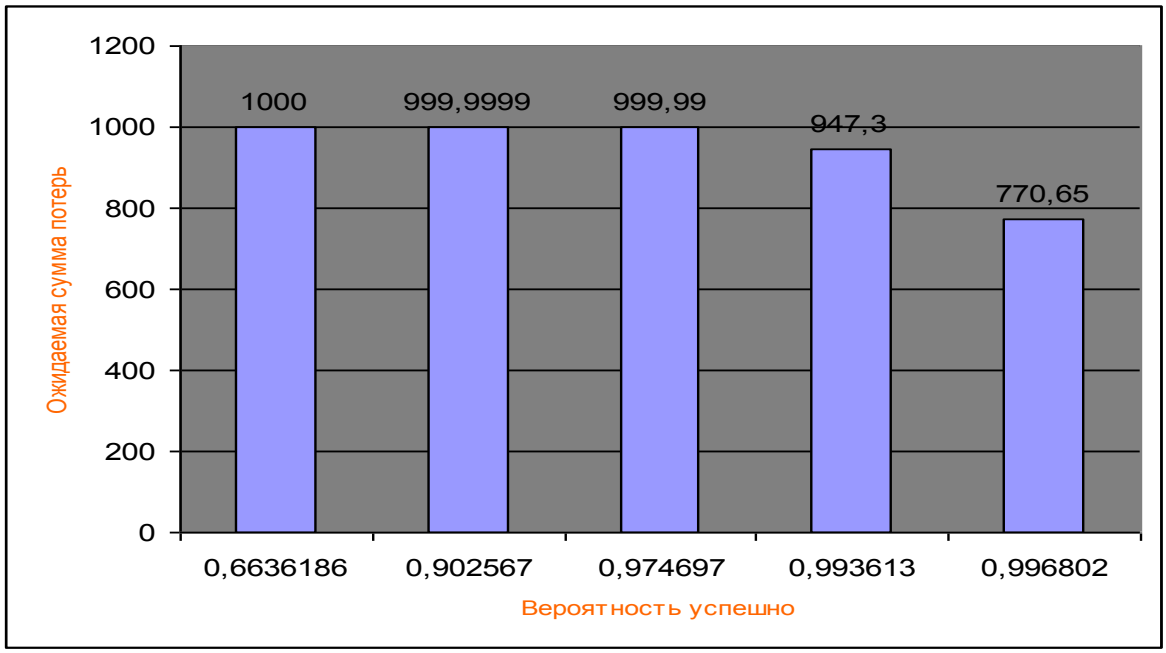



Рис 3.4.5.Зависимость общих потерь системы от вероятности успешного функционирования защиты

Видно, что в условиях длительных атак (даже при восьми-десятикратном повторении угроз) существующая система защиты легко преодолима. Очевидно, в данных условиях ее надо модернизировать.

Б. Рассматривается процедура модернизации системы защиты путем добавления оптимального состава комплекса средств защиты к действующим защитным механизмам.

Если добавляем комплекс средств защиты (табл.3.4.17), которые покрывают всех угрозы, тогда получаем (повторяя методику пункта А данного подраздела):

Таблица.3.4.17. Средства защиты от большинства угроз

| **№ варианта** | **Набор** | **Общая стоимость комплекса средств защиты $** | **Вероятность реализации злоумышленником всех целей** | **Вероятность реализации злоумышленником всех целей с учетом возможности совместного использования средства защиты** |
|---|---|---|---|---|
| **1** | 2, 6, 10 | 1815 | $1.6*10^{-8}$ | $1.6*10^{-8}$ |
| **7** | 3,5,7, 8 | 4189 | $5.42*10^{-13}$ | $5.96*10^{-15}$ |
| **13** | 1,3,4,7,8 | 5785 | $2.42*10^{-15}$ | $3.81*10^{-17}$ |

Таблица 3.4.18. Достижения от вероятности успеха

| **Ср$_{защиты}$** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| **Р$_{успех}$** | 0.93 | 0.85 | 0.87 | 0.9 | 0.76 | 0.6 | 0.46 | 0.9 | 0.3 | 0.9 |
| **Н** защ | 0,07 | 0,15 | 0,13 | 0,1 | 0,24 | 0,4 | 0,54 | 0,1 | 0,7 | 0,1 |
| **Эффект** | **Высокий** | **В** | **В** | **В** | **В** | **В** | **Средний** | **В** | **С** | **В** |

Таблица 3.4.19. Зависимость от наборов средств методов

| **угрозы** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **2,6,10** | **6** | **6** | **6** | **2** | **10** | **6** | **6** | **6** | **6** | **6** | **6** | **6** | **6** | **6** | **6** | **6** | **6** |
| **Н** защ$_{(2,6,10)}$ | 0.4 | 0.4 | 0.4 | 0.15 | 0.1 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 |
| **3,5,7,8** | 3 | 8 | 8 | 5 | 3 | 7 | 8 | 8 | 8 | 7 | 5(7) | 5(7) | 5(7) | 5(7) | 5(7) | 5(7) | 5(7) |
| **Н** защ$_{(3,5,7,8)}$ | 0.13 | 0.1 | 0.1 | 0.24 | 0.13 | 0.54 | 0.1 | 0.1 | 0.1 | 0.54 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 |
| **1,3,4,7,8** | 3 | 8 | 4(8) | 1 | 3 | 7 | 8 | 8 | 8 | 7 | 7 | 7 | 7 | 7 | 1(7) | 1(7) | 1(7) |
| **Н** защ$_{(1,3,4,7,8)}$ | 0.13 | 0.1 | 0.1<br>0.01 | 0.07 | 0.13 | 0.54 | 0.1 | 0.1 | 0.1 | 0.54 | 0.1 | 0.54 | 0.54 | 0.54 | 0.07<br>0.0378 | 0.07<br>0.0378 | 0.07<br>0.0378 |

Таблица 3.4.20. Структурный риск

| Р$_{уя}$ | 0.1 | | 0.05 | | | 0.2 | | 0.15 | | | 0.18 | | 0.3 | | | 0.02 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Р$_{уг}$ | 0.35 | 0.65 | 0.4 | 0.2 | 0.4 | 0.3 | 0.7 | 0.25 | 0.25 | 0.5 | 0.3 | 0.7 | 0.1 | 0.5 | 0.4 | 0.6 | 0.4 |
| Р*риск* | 0.035 | 0.065 | 0.02 | 0.01 | 0.02 | 0.06 | 0.14 | 0.0375 | 0.0375 | 0.125 | 0.054 | 0.126 | 0.03 | 0.15 | 0.12 | 0.012 | 0.008 |
| **Н** защ$_{(2,6,10)}$ | 0.4 | 0.4 | 0.4 | 0.15 | 0.1 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 | 0.4 |
| **Н** защ$_{(3,5,7,8)}$ | 0.13 | 0.1 | 0.1 | 0.24 | 0.13 | 0.54 | 0.1 | 0.1 | 0.1 | 0.54 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 | 0.24<br>0.1296 |
| **Н**защ$_{(1,3,4,7,8)}$ | 0.13 | 0.1 | 0.1<br>0.01 | 0.07 | 0.13 | 0.54 | 0.1 | 0.1 | 0.1 | 0.54 | 0.1 | 0.54 | 0.54 | 0.54 | 0.07<br>0.0378 | 0.07<br>0.0378 | 0.07<br>0.0378 |
| Уровень риска | **Н** | **С** | **Н** | **Н** | **Н** | **С** | **С** | **Н** | **Н** | **С** | **С** | **С** | **Н** | **С** | **С** | **Н** | **Н** |

Таблица 3.4.21. Величина реализации злоумышленником большинства целей

| **Повторная** | **Набор** | **Остаточный риск** | **Потерь $** | **Затрат** | **Стоимость** | **Вероятность реализации злоумышленником** | **Вероятность реализации злоумышленником всех целей с учетом возможности совместного использования средства** |
|---|---|---|---|---|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | **защиты** |
| K=1 | 2,6,10 | 0.4115 | 411.5 | 2911.5 | 1815 | $1.6*10^{-8}$ | $1.6*10^{-8}$ |
| | 3,5,7,8 | 0.259 | 259.49 | 2759.49 | 4189 | $5.42*10^{-13}$ | $5.96*10^{-15}$ |
| | 3,5,(7),8 | 0.204 | 204.25 | 2704.25 | | | |
| | 1,3,4,7,8 | 0.318 | 318.19 | 2818.19 | 5785 | $2.42*10^{-15}$ | $3.81*10^{-17}$ |
| | ,3,4,(7),(8) | 0.312 | 311.882 | 2811.88 | | | |
| K=2 | 2,6,10 | 0.654 | 653.667 | 3153.66 | 1815 | $3.1*10^{-8}$ | $3.1*10^{-8}$ |
| | 3,5,7,8 | 0.452 | 451.585 | 2951.58 | 4189 | $1.08*10^{-12}$ | $1.19*10^{-14}$ |
| | 3,5,(7),8 | 0.367 | 366.781 | 2866.78 | | | |
| | 1,3,4,7,8 | 0.535 | 535.135 | 3035.13 | 5785 | $4.84*10^{-15}$ | $7.63*10^{-17}$ |
| | ,3,4,(7),(8) | 0.526 | 526.493 | 3026.49 | | | |
| K=4 | 2,6,10 | 0.986 | 985.612 | 3485.61 | 1815 | $1.27*10^{-7}$ | $1.27*10^{-7}$ |
| | 3,5,7,8 | 0.909 | 909.544 | 3409.54 | 4189 | $4.33*10^{-12}$ | $4.77*10^{-14}$ |
| | 3,5,(7),8 | 0.839 | 839.226 | 3339.22 | | | |
| | 1,3,4,7,8 | 0.953 | 953.301 | 3453.3 | 5785 | $1.936*10^{-14}$ | $3.05*10^{-16}$ |
| | ,3,4,(7),(8) | 0.949 | 949.730 | 3449.73 | | | |
| K=8 | 2,6,10 | 0.999 | 999.99 | 3499.99 | 1815 | $2.03*10^{-6}$ | $2.03*10^{-6}$ |
| | 3,5,7,8 | 0.999 | 999.99 | 3499.99 | 4189 | $3.47*10^{-11}$ | $3.83*10^{-13}$ |
| | 3,5,(7),8 | 0.999 | 999.99 | 3499.99 | | | |
| | 1,3,4,7,8 | 0.999 | 999.99 | 3499.99 | 5785 | $3.097*10^{-13}$ | $2.46*10^{-15}$ |
| | ,3,4,(7),(8) | 0.999 | 999.99 | 3499.99 | | | |

В результаты получаем:

1- условия $к \in [1,8]$.

1-вариант: при использовании нескольких наборов, например, 1, 7, 13, то в системе появляются потери (411.5 , 259.49 , 318.19 ).

2-вариант с учетом возможности совместного использования средств защиты. : при использовании такого же набора (1, 7, 13) с учётом возможности совместного использования средств защиты, то появляющиеся потери будут меньше, чем в первом варианте (411.5 ,204.25 ,311.88 ).

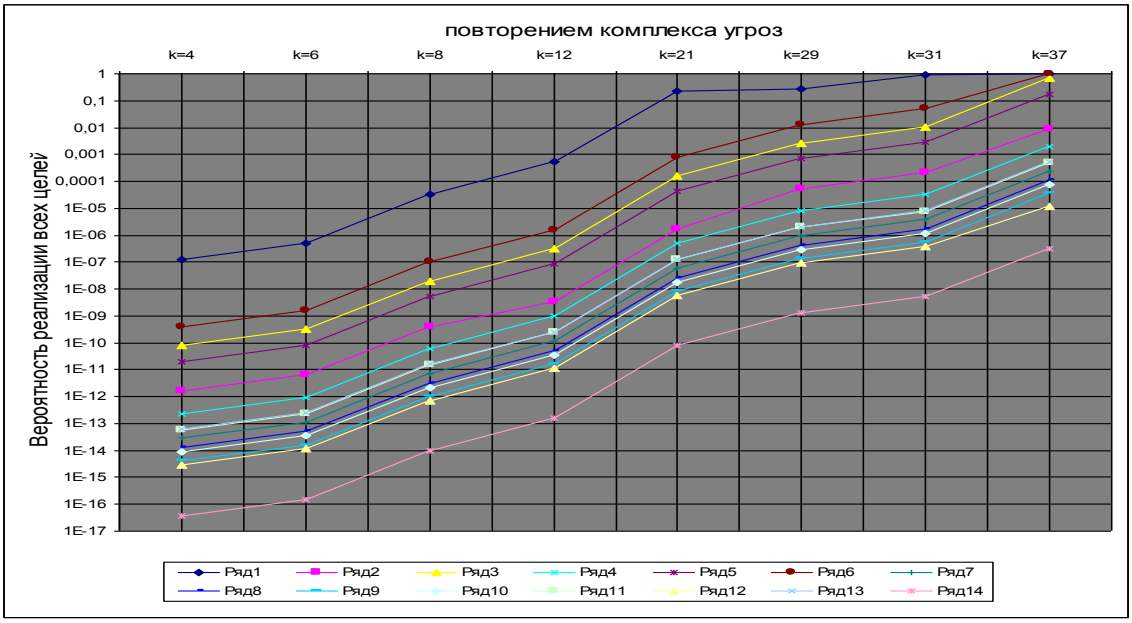
Сравнения между первоначальными средствами защиты, которые были в КИТС ООО «Электроприбор» (г. Москва), и после нашей модернизации приведены в результатах (Потери для всех средств защиты: $О_п$ =1000.

Затраты системы для всех средств защиты: Сзатрат =3500.

Результаты представлены в табл.(3.4.22-23) на рис.(3.4.6а , 3.4.6б).

Таблица 3.4.22. Совместное использование

| № варианта | Набор | Общая стоимость комплекса средств защиты | Вероятность реализации злоумышленником всех целей | | | |
|---|---|---|---|---|---|---|
| | | | K=21 | K=29 | K=31 | K=37 |
| **1** | 2, 6, 10 | 1815 | 0,235 | 0,2686 | 0,918 | 0,999 |
| **2** | 2, 3,7,8,9 | 3029 | 1,66E-06 | 5,335E-05 | 2,13E-04 | 0,0088 |
| **3** | 3, 5, 6 | 3285 | 0,000166 | 0,00266 | 0,0106 | 0,669 |
| **4** | 2,3,4,7, 8 | 3439 | 5,01E-07 | 8,019E-06 | 3,21E-05 | 0,00196 |
| **5** | 2, 3, 5, 6 | 3535 | 4,32E-05 | 0,00069 | 0,0027 | 0,1689 |
| **6** | 1, 6, 10 | 4065 | 0,00081 | 0,01299 | 5,09E-02 | 0,956 |
| **7** | 3, 5, 7, 8 | 4189 | 5,956E-08 | 9,53E-07 | 3,81E-06 | 0,00023 |
| **8** | 3,5,7,8, 9 | 4279 | 2,64E-08 | 4,23E-07 | 1,69E-06 | 0,00011 |
| **9** | 2,3,5,7, 8 | 4439 | 8,514E-09 | 1,36E-07 | 5,45E-07 | 3,49E-05 |
| **10** | 3,4,5,7, 8 | 4689 | 1,812E-08 | 2,89E-07 | 1,16E-06 | 7,4E-05 |
| **11** | 1,3,7,8, 9 | 5529 | 1,21803E-07 | 1,94884E-06 | 7,80E-06 | 0,00049 |
| **12** | 1, 3, 5, 6 | 5539 | 5,956E-09 | 9,53E-08 | 3,81E-07 | 1,22E-05 |
| **13** | 1,3,4,7, 8 | 5785 | 1,302E-07 | 2,08E-06 | 8,33E-06 | 0,00054 |
| **14** | 1,3,5,7, 8 | 6939 | 8,032E-11 | 1,29E-09 | 5,14E-09 | 3,29E-07 |



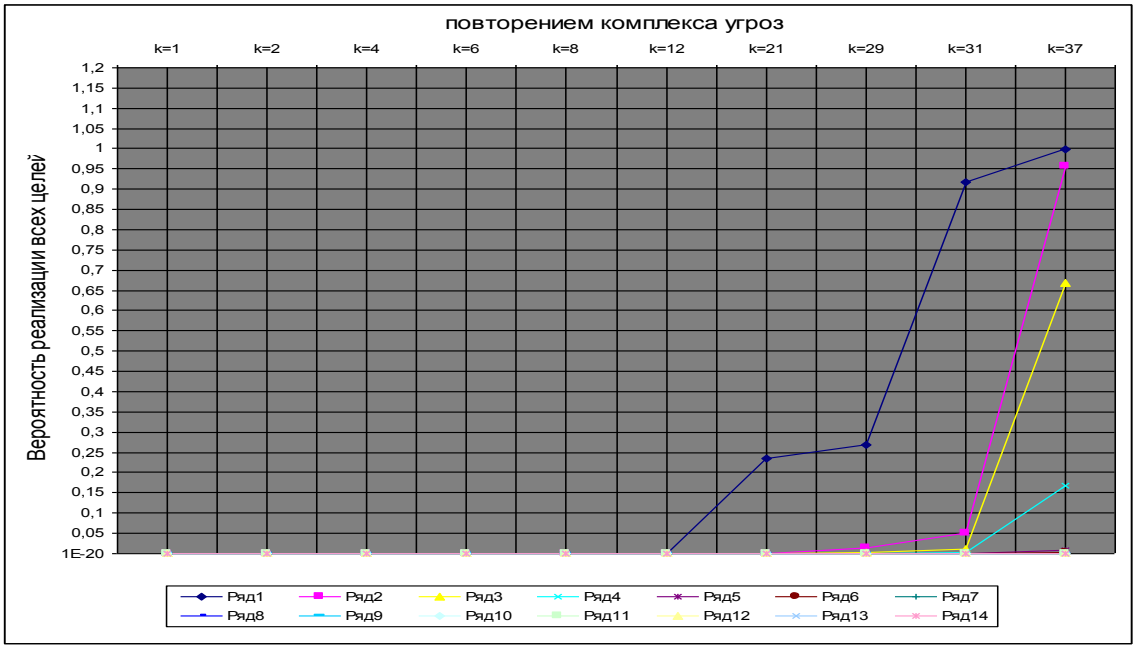



Рис.3.4.6.

Результаты:

После К=29 диаграмма № 1,3,6 стала приближаться к 1. Проведем сравнение между вероятностями угроз на примере диаграмм, каждая из которых имеет набор защит.

Наборы защит диаграмм удалённых от 1 являются более сильными, чем наборы защит диаграмм, приближённых к 1, так как у удалённых – вероятность угроз меньше.

Поэтому, мы будем использовать набор защит диаграммы № 14 для всех целей злоумышленника.

Таблица 3.4.23. Совместное использование средств защиты

| **№ варианта** | **Набор** | **Общая стоимость комплекса средств защиты** | **Вероятность реализации злоумышленником всех целей** | **Вероятность реализации злоумышленником всех целей с учетом возможности совместного использования средства защиты** |
|---|---|---|---|---|
| 1 | 2, 6, 10 | 1815 | 1,28E-07 | 1,28E-07 |
| **2** | 2, 3,7,8,9 | 3029 | 7,98E-10 | 1,59E-12 |
| **3** | 3, 5, 6 | 3285 | 2,43E-09 | 7,91E-11 |
| **4** | 2,3,4,7, 8 | 3439 | 7,98E-10 | 2,39E-13 |
| **5** | 2, 3, 5, 6 | 3535 | 1,52E-09 | 2,06E-11 |

| | | | | |
|---|---|---|---|---|
| **6** | 1, 6, 10 | 4065 | 5,6E-08 | 3,87E-10 |
| **7** | 3, 5, 7, 8 | 4189 | 4,33E-12 | 2,84E-14 |
| **8** | 3,5,7,8, 9 | 4279 | 4,33E-12 | 1,26E-14 |
| **9** | 2,3,5,7, 8 | 4439 | 2,712E-12 | 4,06E-15 |
| **10** | 3,4,5,7, 8 | 4689 | 4,33E-12 | 8,64E-15 |
| **11** | 1,3,7,8, 9 | 5529 | 1,004E-11 | 5,808E-14 |
| **12** | 1, 3, 5, 6 | 5539 | 1,2E-12 | 2,84E-15 |
| **13** | 1,3,4,7, 8 | 5785 | 2,52E-10 | 6,208E-14 |
| **14** | 1,3,5,7, 8 | 6939 | 1,2E-12 | 3,83E-17 |

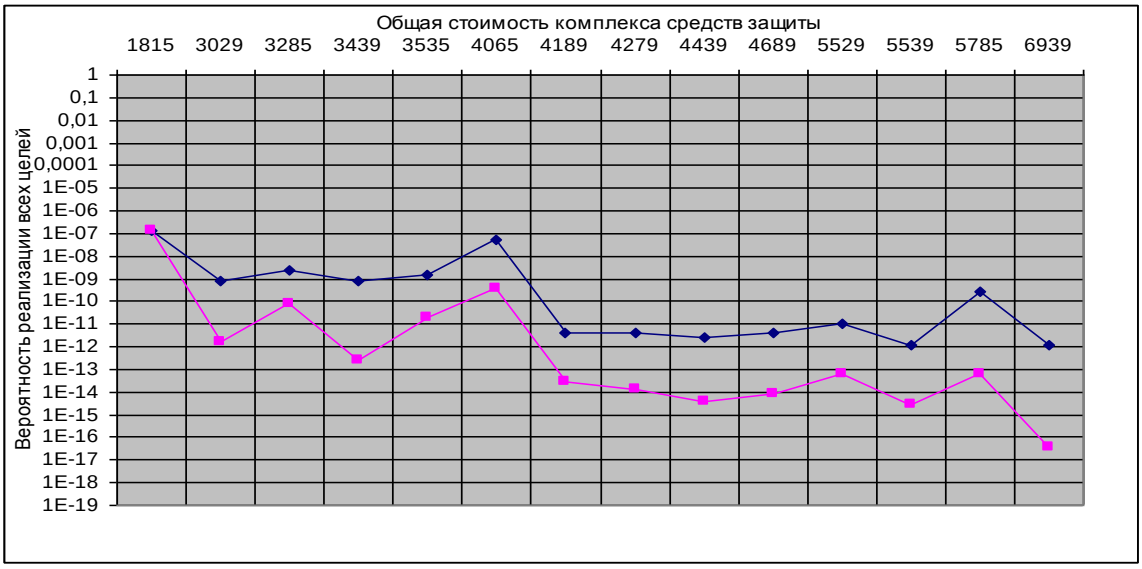



Рис.3.4.7. Велечины достижения злоумышленником всех целей от стоимости комплекса средств защиты (всех целей диаграммы № 1, диаграммы № 2, с учетом возможности совместного использования защиты)

На рис.3.4.8. приведены сравнения вероятности реализации злоумышленником своих целей для известной и предлагаемой, разработанной системы защиты в условиях многократной атаки

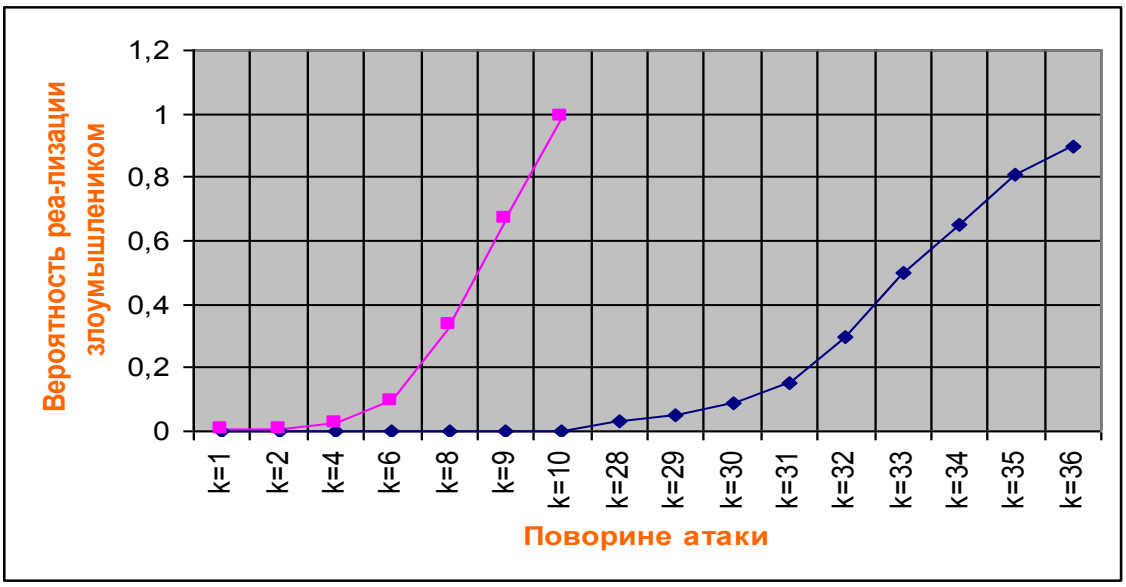



Рис. 3.4.8. Вероятность реализации злоумышленником для известных средств и разработанного варианта защиты

**Определение уровня риска на основе нечеткой логики.** Для определения рисков можно, оставаясь в рамках трехбалльной шкалы, выбрать для вероятностей реализации угроз значения 0.1 (низкая), 0.5 (средняя) и 1.0 (высокая), а для уровней воздействия — 10, 50 и 100. Тогда, если произведение вероятности на воздействие не превосходит 10, риск можно считать низким. Значения от 10 до 50 соответствуют умеренному риску, свыше 50 — высокому.

При низком риске следует решить, нужны ли какие-то корректирующие действия, или можно принять риск.

Умеренный риск также требует планирования, и реализации корректирующих действий за разумный период времени. КИТС описываемая четыре параметрами: угроза, уязвимость, риск , комплекс средств защиты.

Высокий риск требует незамедлительного планирования и реализации корректирующих действий. Если по какой-либо причине планирование или реализация затягиваются, может ставиться вопрос о приостановке работы КИТС или ее частей.  Все показатели  легко измеряются и множество

возможных значений доступно.

Из нашего опыта работы с системой получены правила, связывающие значения этих параметров.

**Описание логико-лингвистической модели “уверенность риска”**

Приводим описание нечёткой системы принятия решения о необходимости защиты КИТС с применением ИСППР.

Первые три лингвистических переменных являются входными, – уверенность риска выходная переменная правил. Правила системы определяются следующей табл.3.4.24:

Таблица 3.4.24. Логико-лингвистические модели и правила системы нечеткой логики в ИСППР

| Входные лингвистические переменные | | | Выходная линг. переменная |
|---|---|---|---|
| Уязвимость | Угроза | К защ | Уверенность риска |
| низкая | Низкая | Очень низкая | Очень низкая |
| низкая | Высокая | Низкая | Низкая |
| низкая | Низкая | Низкая | Низкая |
| низкая | Очень низкая | Нет | Очень низкая |
| низкая | Низкая | Нет | Очень низкая |
| низкая | Низкая | Нет | Очень низкая |
| низкая | Высокая | Нет | Низкая |
| низкая | Очень низкая | Нет | Очень низкая |
| низкая | Очень низкая | Нет | Очень низкая |

| | | | |
|---|---|---|---|
| низкая | Средняя | Нет | Низкая |
| низкая | Низкая | Средняя | Низкая |
| низкая | Высокая | Средняя | Средняя |
| низкая | Очень низкая | Средняя | Низкая |
| низкая | Средняя | Средняя | Низкая |
| Низкая | Низкая | Средняя | Низкая |
| Очень низкая | Высокая | Средняя | Низкая |
| Очень низкая | Низкая | Средняя | Низкая |

Каждое из правил представляет из себя нечёткую импликацию для конкретной структуры или конкретных заданий.

При преобразовании нечётких множеств любое правило содержащее в левой части как конъюнкции, так и дизъюнкции можно привести к системе правил, в левой части каждого будут либо только конъюнкции, либо только дизъюнкции. Таким образом, не уменьшая общности, можно рассматривать правила, содержащие в левой части либо только конъюнкции, либо только дизъюнкции.

Если сломался датчик, измеряющий значение одного из параметров системы, но знать его значение необходимо. Тогда встаёт задача об отыскании значения этого неизвестного значения (пусть это будет уверенность риска) при известных значениях три других параметров (угроза, уязвимость, и комплекс средств защиты (К защ. ).

Используя один из способов построения нечёткой импликации мы получим новую нечёткую переменную, соответствующую степени уверенности о значении выходного значения при применении к заданным входным соответствующего правила. Степень уверенности посылки мы вычислили, а степень уверенности заключения задаётся функцией

принадлежности соответствующего терма.

Объединение результатов применения всех правил - аккумуляция. Один из основных способов аккумуляции – построение максимума полученных функций принадлежности. Получаем:

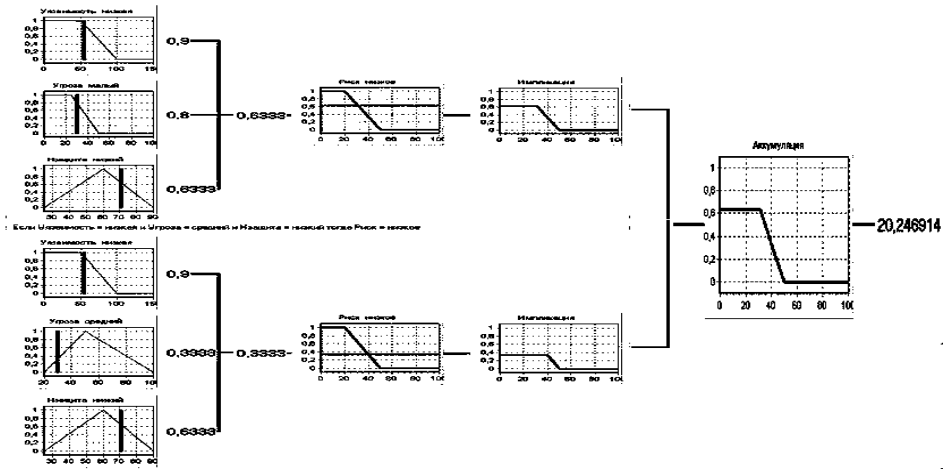



Рис.3.4.9. Процесс нечёткого вывода в ИСППР

Когда необходимо, какое то конкретное числовое значение, то для его получения используется этап дефаззификации, т.е. получения конкретного значения из универса по заданной на нём функции принадлежности.

Полученную функцию принадлежности уже можно считать результатом. Это новый терм выходной переменной риска. Функция принадлежности говорит о степени уверенности в значении риска при заданных значениях входных параметров и правилах, определяющих соотношение входных и выходных переменных, которые, как правило, задаются заказчиком.

Существует множество методик дефаззификации, но нам достаточно метода первого максимума. Применяя его к полученной функции принадлежности, получаем, что значение уверенность риска 20,25 (низкий)[26-28, 101,102,107-110].

## 3.5. Информационная защита сетевых соединений банковских КИТС Палестины

Нами в ходе исследований конкретных КИТС установлена недостаточность защиты сетевых соединений между рабочими станциями и

серверами, организованных посредством интерфейса NPFS(пока основной в Палестине). Этот интерфейс имеет ряд недостатков, позволяющих осуществлять различные удаленные атаки[51]. Предложены и рассмотрены две атаки, одна из которых относится к классу "отказ в обслуживании", а другая позволяет получать обычному пользователю права администратора путем перехвата административных сетевых соединений.

Создание канала происходит следующим образом. Процесс-сервер создает канал с помощью функции программного интерфейса Win32 CreateNamedPipe[9,51]. Канал может быть создан только на локальном компьютере.

Драйвер npfs.sys, хотя и работает в соответствии со спецификациями драйвера файловой системы, не управляет никакими файлами. Вместо этого npfs.sys управляет так называемыми каналами (named pipes). Вместе с файлами, дисковыми директориями, устройствами и почтовыми ящиками (mailslots) каналы относятся к классу файловых объектов.

Интерфейс NPFS имеет другие возможности: поддерживаются асинхронная передача информации, транзакции и многое другое. С помощью NPFS решается множество задач, некоторые из которых играют важную роль в обеспечении безопасности операционной системы. Например, каналы lsass, lsarpc и LANMAN используются при передаче по сети имени и пароля пользователя при сквозной аутентификации в домене КИТС.

Предложим возможности усиления информационной защиты NPFS-соединений, которые разместим в табл.3.5.1.

Таблица 3.5.1. Взаимосвязи в КИТС при защитных мероприятиях с ПО

| Применения | | Средства достижения эффекта | | |
|---|---|---|---|---|
| Клиент | Канал | Драйвер | Файл | Интерфейс |
| КИТС без защиты | named pipes | npfs.sys | NPFS | impersonation |

| | | | | |
|---|---|---|---|---|
| домен КИТС с защитой | mailslots | PipeBomb | CreateFile, ReadFile WriteFile | impersonation |
| computer_ namepipepipe_ name | Win32 CreateNamedPipe | security descriptor | NPFS | Win32 CreateNamed Pipe |
| Lsarpc | CloseHandle | thread | NPFS | impersonation |
| Сервер LSA | DisconnectNamedPipe | ReadFile | ConnectNamed Pipe | impersonation |
| Guest, admin | lsass | thread | CreateFile | Win32 CreateNamed Pipe |
| домен КИТС с защитой, Сервер LSA | LANMAN AdminTrap | PipeBomb | CreateFile, ReadFile WriteFile | Win32 CreateNamed Pipe |

Примечание: NPFS расшифровывается как Named Pipe File System[9,51,100,109]. Несмотря на то, что в этом названии присутствуют слова "file system", назвать NPFS файловой системой можно только в первом приближении. Это более широкое понятие хорошо видно из таблицы.

Сервер может отключить клиента в любой момент с помощью функции DisconnectNamedPipe, а вот клиент может отключиться от канала только с помощью функции CloseHandle[51].

После прекращения связи с клиентом сервер может повторно использовать канал с помощью повторного вызова функции ConnectNamedPipe. Когда клиент КИТС банка подключается к каналу, операционная система предоставляет ему первый экземпляр, поскольку он был создан раньше. Но когда к тому же каналу захочет подключиться другой клиент, он будет подключен ко второму экземпляру.

При этом клиент банка никакими средствами не сможет определить, какой процесс обслуживает его запрос[51]. Получается, что клиент хотел

получить услугу от одного процесса, а на самом деле эту услугу ему предоставляет совсем другой процесс. Это может быть опасным в банковской сфере.

Нами экспериментально установлено, что пользователь guest с помощью обычной прикладной программы может открывать системный канал lsass и записывать туда все, что угодно. Видно, что NPFS представляет собой объект для удаленных атак. Однако, как показали наши эксперименты[104.105], более вероятна другая картина.

Обычно, когда процесс-сервер понимает, что все экземпляры его канала заняты, этот процесс начинает создавать новые экземпляры канала.

Для повышения эффективности использования нечеткой логики, для ускорения проведения экспертных оценок нами использовались ПЛИС.

Приведем один из алгоритмов, который использован при проектировании сети с нечеткой логикой. Он позволяет быстрее разработать программы ПЛИС с защитой сети от проникновений и защитить телекоммуникации клиент-сервер (рис.3.5.1).

Это позволит устранить эффекты, которые приводят к тому, что загрузка процессора компьютера, на котором выполняется процесс-сервер, стабильно держится на уровне 100% (при этом около 90% времени процессор обслуживает процессы с базовым приоритетом High), а объем свободной оперативной памяти этого компьютера уменьшается со скоростью от 1 до 3 мегабайт в секунду.

С помощью этого алгоритма можно ускорить процедуру олицетворения, одну из важных функций нечеткой логики.

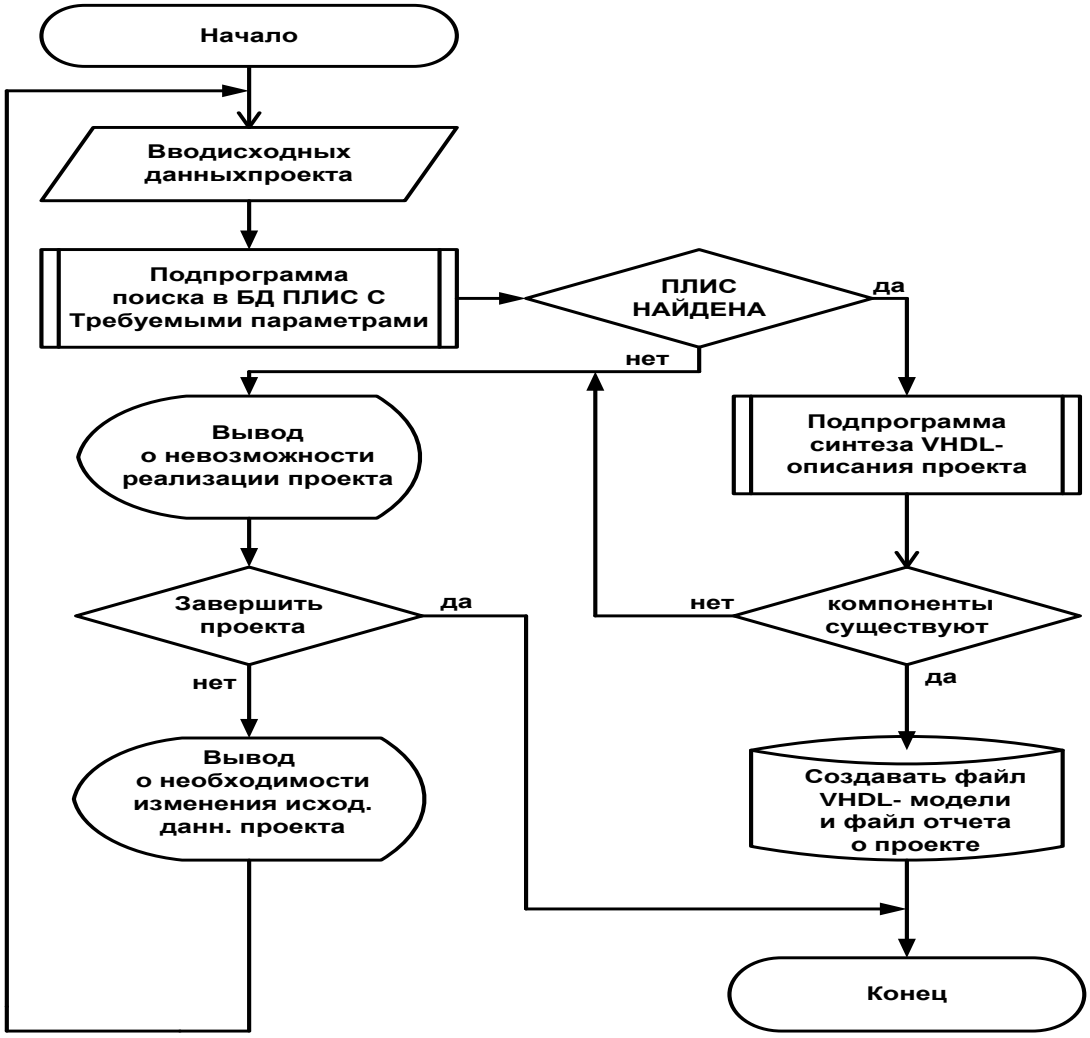



Рис.3.5.1. Блок-схема алгоритма процесса автоматизированного синтеза программы экспертной оценки и олицетворения в КИТС

Должно быть запрещено создание процессом экземпляра канала, для которого уже существует экземпляр, созданный другим процессом. Это может быть сделано с помощью драйвера фиктивного устройства, фильтрующего информационные потоки, проходящие через драйвер npfs.sys.

Указанная атака характерна тем, что использует не слабости протокола TCP/IP, а недостатки своего программного обеспечения этой операционной системы. Атака одинаково эффективно поражает и рабочие станции, и серверы. Для демонстрации того, что программа AdminTrap действительно получает полномочия пользователя, соединение с которым она перехватила, нами была выбрана [109] нестандартная процедура, а именно: учетная запись пользователя AdminTrap, созданная программой, не

может использоваться для несанкционированного доступа к ресурсам операционной системы без дополнительных действий, выполнить которые может только администратор.

Наши апробированные рекомендации сетевому администратору банка, который применяет конкретную КИТС с заказанной защитой сведены нами в табл.3.5.2:

Таблица 3.5.2. Разработанные нами рекомендации сетевому администратору

| Действие | Кто выполняет |
|---|---|
| в Setup разрешить загрузку только с жесткого диска | Администратор сети |
| установить пароль на вход в Setup | Администратор сети, операционист, клиент, партнер |
| использовать файловую систему NTFS | Администратор сети, операционист, |
| запретить или максимально ограничить доступ к компьютеру через сеть | Администратор сети, |
| активизировать служебную программу SYSKEY | Администратор сети, операционист, |
| включить использование аутентификации только по запросу сервера | Администратор сети, операционист, партнер |

Программно и логически это можно записать с помощью следующих значений:

0x00000010 - целостность сообщения;

0x00000020 - конфиденциальность сообщения;

0x00080000 - NTLMv2 защита сеанса;

0x20000000 - 128-битное шифрование.

• при выборе паролей необходимо соблюдать следующие правила:

• ни в коем случае не выбирать в качестве пароля или части пароля любое слово, которое может быть в каком-либо словаре, или его модификацию;

• пароль должен быть длиной минимум 7 символов, но желательнее 14 (максимально возможная длина пароля);

• каждая из 7-символьных половин пароля должна содержать символы из возможно большего символьного набора;

• соблюдать прочие правила администрирования, помня о том, что существуют и другие методы взлома операционной системы.

Active Directory (AD) — это ключевой компонент КИТС, позволяющий решить характерные проблемы масштабируемости, расширяемости, администрирования и открытости. Это приспособлено в полной мере для работы в крупных организациях, поскольку число пользователей домена не может превышать 20 000(хорошо соблюдается в Палестине).

Служба AD существенно расширяет возможности администрирования.

Шифрование. Единственный надежный способ защиты размещенной на жестком диске в банке или в КИТС конфиденциальной информации — шифрование. При этом кодирование и декодирование выполняются абсолютно прозрачно для пользователя и приложения, под надзором администратора, что позволяет защитить данные любой прикладной программы, обслуживающей конкретную КИТС. IPSec — это надежный протокол Интернет, имеющий сильную отраслевую поддержку в Палестине.

Для него удобно разрабатывать процесс экспертной оценки характеристик КИТС с учетом особенностей пользователей и клиентов и квалификации экспертов.

В процессе наших исследований и внедрений нами разработаны рекомендации: как защититься от вредоносного определения IP в КИТС и клиентского и сотрудников банков:

1) запретить cookies, запретить выполнение активных сценариев, запретить Java, запретить ActiveX;

2) использовать Socks-ификацию браузера. При этом вся информация, которую отправляет и принимает браузер (или другая программа), «перехватывается» и направляется на прокси сервер.

Для упрощения и ускорения использования этого подхода нами разработана программа, время действия, которой несколько секунд.

Программа для выработки активных сценариев по поиску ПЛИС:

```
// aaaa.cpp: определяет точку входа для консольного приложения.
//
#include "stdafx.h"
#include <iostream>
#include <string>
using std::cout;
using std::cin;
using std::endl;
int main()
{
	int arr[10];
	// Заполняем массив с клавиатуры
	for (int i = 0; i < 10; i++) {
	    cout << "[" << i + 1 << "]" << ": ";
	    cin >> arr[i];
	}
	// И выводим заполненный массив.
	cout << "\nВаш массив: ";

	for (int i = 0; i < 10; ++i) {
	    cout << arr[i] << " ";
	}
	cout << endl;
	return 0;
}// stdafx.cpp: исходный файл, содержащий только стандартные включаемые модули
// aaaa.pch будет предкомпилированным заголовком
// stdafx.obj будет содержать предварительно откомпилированные сведения о типе
```

```
#include "stdafx.h"
// TODO: Установите ссылки на любые требующиеся дополнительные заголовки в файле STDAFX.H
// , а не в данном файле
// stdafx.h: включаемый файл для стандартных системных включаемых файлов
// или включаемых файлов для конкретного проекта, которые часто используются, но
// не часто изменяются
//
#pragma once
#include "targetver.h"
#include <stdio.h>
#include <tchar.h>
// TODO: Установите здесь ссылки на дополнительные заголовки, требующиеся для программы
```

==========

КОНСОЛЬНОЕ ПРИЛОЖЕНИЕ. Обзор проекта аааа

==========

Это приложение аааа создано автоматически с помощью мастера приложений.

Здесь приведены краткие сведения о содержимом каждого из файлов, использованных при создании приложения аааа.

аааа.vcxproj

Основной файл проекта VC++, автоматически создаваемый с помощью мастера приложений.

Он содержит данные о версии языка Visual C++, использованной для создания

файла, а также сведения о платформах, настройках и свойствах проекта,

выбранных с помощью мастера приложений.

aaaa.vcxproj.filters

Это файл фильтров для проектов VC++, созданный с помощью мастера

приложений.

Он содержит сведения о сопоставлениях между файлами в вашем проекте и

фильтрами. Эти сопоставления используются в среде IDE для группировки

файлов с одинаковыми расширениями в одном узле (например файлы ".cpp"

сопоставляются с фильтром "Исходные файлы").

aaaa.cpp

Это основной исходный файл приложения.

////////////////////////////////////////////////////////////////////////////

Другие стандартные файлы:

StdAfx.h, StdAfx.cpp

Эти файлы используются для построения файла предкомпилированного заголовка

(PCH) с именем aaaa.pch и файла предкомпилированных типов

с именем StdAfx.obj.

////////////////////////////////////////////////////////////////////////////

Общие замечания:

С помощью комментариев «TODO:» в мастере приложений обозначаются фрагменты

исходного кода, которые необходимо дополнить или изменить.

////////////////////////////////////////////////////////////////////////////

#pragma once

```
// Включение SDKDDKVer.h обеспечивает определение самой последней доступной платформы Windows.
// Если требуется выполнить построение приложения для предыдущей версии Windows, включите WinSDKVer.h и
// задайте для макроса _WIN32_WINNT значение поддерживаемой платформы перед включением SDKDDKVer.h.
#include <SDKDDKVer.h>
```

Приведем один из разработанных интерфейсов для «Банка Палестина»:

```
library IEEE;
use IEEE.std_logic_1164.all;
use IEEE.std_logic_arith.all;

entity FSK is
        generic( CODEWIDTH          :integer := 15;
                PHASEWIDTH          :integer := 10;
                SINWIDTH        :integer := 8;
                TuningWord1: std_logic_vector(CODEWIDTH-1 downto 0);
                TuningWord2: std_logic_vector(CODEWIDTH-1 downto 0));
        port(  clk: in std_logic;
                reset: in std_logic;        DataIn: in std_logic;
                OutSignal: out std_logic_vector(7 downto 0)        );
end FSK;
```

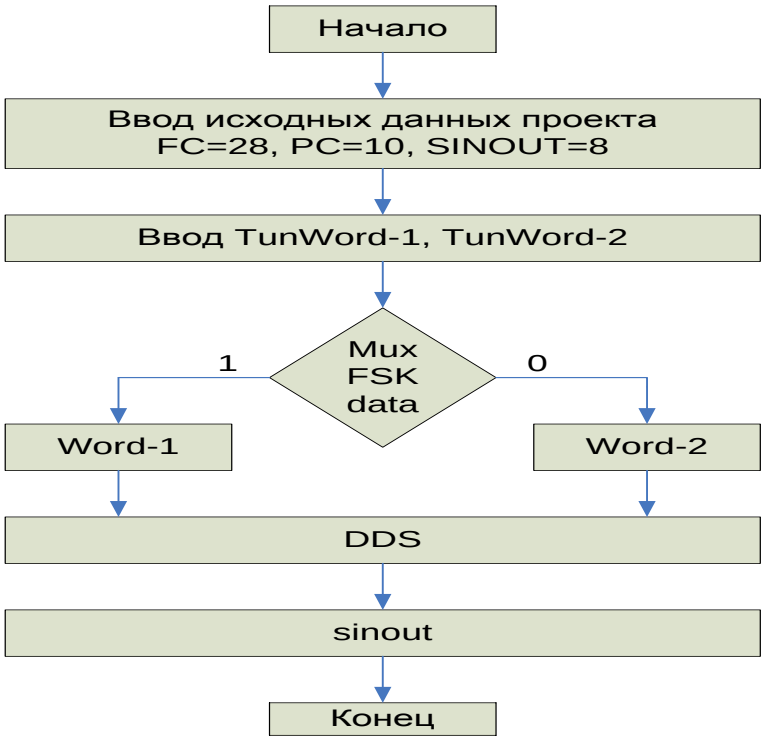



Рис. 3.5.2.Алгоритм работы интерфейса

Напоминаем  важное (получено нами опытным путем при внедрении этих программ на конкретных предприятиях):

- любой прокси-сервер ведет журнал своей работы, в котором подробно расписано, какой IP-адрес в какое время куда обращается.

- Пользователь (в том числе, и злоумышленник), который располагает соответствующими полномочиями и запасом времени, всегда сможет выяснить, ваши передвижения по сети, даже если  будет использоваться цепочки из многих анонимных прокси- серверов в разных регионах Палестины и даже за рубежом.

- Задача администраторов защиты: не допустить этого. То, что это выполняется с помощью наших методик, мы убедились при внедрениях(см. приложения).

## Выводы по главе 3

1. Предложен новый подход к нечеткому структурно-логическому обобщению знаний на основе нечеткой геометрической интерпретации данных и знаний с главным преимуществом – отличие от символьных логических методов обобщения знаний, опирающихся на эвристические соображения и не имеющих строгого обоснования.
2. Разработана методика и сделана минимизация маршрутизаторов в конкретной сети с обеспечением защиты.
3. Разработана методика нечеткой идентификации, к задаче обнаружения олицетворения при запросах доступа к ресурсам КИТС.
4. Разработаны методики и программные модули в среде Delphi 4, которые позволили провести тестирование нечетких алгоритмов принятия решений в задачах управления в условиях неопределенности. Результаты тестирования этих модулей на реальных данных формирования и некоторых предприятий (НПО «РИК», г. Владимир; ООО «Электроприбор», г. Москва) повысили их эффективность (на 70%) по сравнению с традиционными методами принятия управленческих решений и позволили повысить их конкурентоспособность, они отвечают современному направлению развития интеллектуальных систем – мягким вычислениям.

## Заключение

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

1. В условиях Палестины жизненно необходима защита корпоративных и банковских сетей.
2. Поскольку существует большая неопределенность во многих ситуациях различных угроз, проникновений и возможной защиты от них, то целесообразно применения аппарата нечеткой логики.
3. Разработаны модели, методики, алгоритмы и структуры для корпоративных и банковских защищенных сетей применительно к условиям Палестины.
4. Разработана структура ИСППР для диагностики состояния КИТС, реализующая проведение сигнатурного и статистического анализа сетевого трафика и работу НИС реагирования на нештатные сетевые ситуации.
5. Результаты экспериментальной проверки разработанных моделей и алгоритмов оптимизации состава средств защиты и управления безопасностью на основе анализа рисков показали их работоспособность и практическую значимость.
6. На этой основе выработаны рекомендации и предложения по созданию новых и усовершенствованию существующих систем защиты информации в КИТС завода «Электроприбор» (г. Москва) (аналогичный по сетевой структуре палестинским банковским сетям). Обеспечивают выигрыш по сравнению с существующими на 70%.
7. Предложен новый подход к нечеткому структурно-логическому обобщению знаний на основе нечеткой геометрической интерпретации данных и знаний с главным преимуществом – отличие от символьных логических методов обобщения знаний, опирающихся на эвристические соображения и не имеющих строгого обоснования.
8. Разработана методика и сделана минимизация маршрутизаторов в

конкретной сети с обеспечением защиты.

9. Разработана методика нечеткой идентификации, к задаче обнаружения олицетворения при запросах доступа к ресурсам КИТС.
10. Разработаны методики и программные модули в среде Delphi 4, которые позволили провести тестирование нечетких алгоритмов принятия решений в задачах управления в условиях неопределенности. Результаты тестирования этих модулей на реальных данных формирования и некоторых предприятий (НПО «РИК», г. Владимир; ООО «Электроприбор», г. Москва) повысили их эффективность (на 70%) по сравнению с традиционными методами принятия управленческих решений и позволили повысить их конкурентоспособность, они отвечают современному направлению развития интеллектуальных систем – мягким вычислениям.

ЛИТЕРАТУРА

1. Галкин А.П. Защита каналов связи предприятий и учреждений от несанкционированного доступа к информации./Уч. пос.- Владимирский государственный университет.- г. Владимир-2003. 126 с.

2. Галкин А.П. Информационная безопасность и целесообразные пути ее улучшения/ Palmarium Academic Publishing - Saarbrucken, Deuchland - 2014. 75 с.

3. Darahma I .The main tasks of designing a secure network-on-chip/Galkin A.P., Aljaradat M.M.., Amro M.M.//Indian Science Cruiser. 2014, v. 28. N. 4. P.41-43.

4. Гост 20.911-89, Техническая диагностика. Основные термины и определения. - М.: Стандарты, 1990.

5. Амато В. Основы организации сетей Cusco, том 1.-М.; Издательский дом “Вильямс”, 2002, 512 с.

6. Афанасьев В.Б., Безроднов В.И., Давыдов А.А. Исследование корректирующих кодов для контроля дисплея // Помехоустойчивое кодирование и надежность ЭВМ. М.: Наука. 1987, С. 151-186

7. Александрович А.Е. Разработка методов и средств обеспечения и анализа надежности отказоустойчивых вычислительных систем. /Диссертация на соискание ученой степени к.т.н. 61: 96- 5/ 807-х, М.: 1994, 163 с.

8. Барановская Т.П., Лойко В.И., Семенов М.И., Трубилин А.И. Архитектура компьютерных систем и сетей. - М.: Финансы и статистика, 2003, 256 с.

9. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации./ Учебник для вузов. 2-е изд. - СПб.: Питер, 2006, - 703 с

10. Бройдо В. Вычислительные системы, сети и телекоммуникации. / Учебник для вузов. 3-е изд.- СПб.: Питер, 2008, -768 с.

11. Васильев В.Н., Стафеев С.К., Селиверстов А.В., Мельничук А.П. Федеральный естественнонаучный образовательный портал как часть единой интернет-системы «Российское образование» // Телематика-2003:

Труды X всерос. науч.-метод. конф. СПб., 2003. - С. 207.

12. Васильков Ю.В. Проблемы качества обучения с использованием электронных учебников // Электронные учебники и электронные библиотеки в открытом образовании: Тез. докл. 2-й всерос. конф. М.: «МЭСИ», 2001. С. 110-116

13. Гиркин И.В. Новые подходы к организации учебного процесса с использованием современных компьютерных технологий // Информационные технологии", 1998, №6. - С. 44-47.

14. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания.- М.: Наука. Гл. ред. физ.-мат. лит. - 1987.- 520 с.

15. Гусев П.В. Построение современной концептуальной модели системы корпоративного обучения на основе распределенной среды дистанционного обучения Learning Space 4.0 // Телематика-2001: Труды междунар. науч.- метод. конф. СПб., 2001.-С. 81.

16. Дунаев С. Доступ к базам данных и техника работы в сети. Практические приемы современного программирования. — М.: ДИАЛОГ-МИФИ, 1999.- 416 с.

17. Галкин А.П. Проектирование эффективной сети связи с учетом срывов/ Проектирование и технология электронных средств.-2003-№1, с.9-11.

18. Галкин А. П. Целесообразность информационной защиты предприятия./ Материалы 3-ей Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир, 1999, с.64-67.

19. Галкин А. П. Оценка необходимости защиты информации предприятия. «Вестник ассоциации Русская оценка»,1999-1, с.55-58.

20. Галкин А. П. Зависимость эффективности сети связи от срывов. / Материалы 4-ой Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир-Суздаль, 2001, с.72-77.

21. Галкин А.П., Аль-Муриш Мохаммед, Тахаан Осама. Обнаружения атак и нарушений в корпоративной сети./ Экономические проблемы ресурсного

обеспечения инновационного развития региона. Матер.междунар. научн. конф. Владимир, 2009. С.15-19.

22. Галкин А.П., Аркадьева М.С., Тахаан Осама. Кризис, безработица и информационная безопасность предприятия./ Экономические проблемы ресурсного обеспечения инновационного развития региона. Матер.междунар. научн. конф. Владимир, 2009. С.20-24.

23. Галкин А.П., Аль-Муриш Мохаммед, А.В. Дерябин -Нечеткий вывод, нечеткая логика и их применение при информационной защите систем // Известия института инженерной физики. 2009-№2.-С.13-15.

24. Галкин А.П., Тахаан Осама. Выбор комплекса защиты информации для корпоративных информационно-телекоммуникационных сетей./ Известия института инженерной физики. 2010-№2. С. 2-6.

25. Галкин А.П. Радиосистемы для защиты каналов связи от несанкционированного доступа к информации: Учеб. пособие / Владим. гос. ун-т. Владимир, 2003. 104 с.

26. Галкин А.П. Информационная безопасность и целесообразные пути её улучшение// Palmarium Academic Publishing . Saarbruken,Deuchland, 2014. 75 с.

27. Галкин А.П., Тахаан Осама. Информационная защита корпоративной сети системой обнаружением атак с нечеткой логикой./ Известия института инженерной физики. 2009-№4. С. 2-4.

28. Галкин А.П., Тахаан Осама. Выбор комплекса защиты информации для корпоративных информационно-телекоммуникационных сетей./ Известия института инженерной физики. 2010-№2. С. 2-6.

29. Денисова А., Вихарев И., Белов А., Наумов Г. Интернет. 2-е изд. – СПб. Питер. 2004.– 368 с.

30. Давыдов А.А., Дрожжина-Лабинская А.Ю. Дополнительные корректирующие возможности кодов БЧХ, исправляющих двойные и обнаруживающие тройные ошибки. // Вопросы кибернетики. Комплексное

проектирование элементно-конструкторской базы супер-ЭВМ. М.: ВИНИТИ, 1988. С. 86-112.

31. Доманицкий С.М. Построение надежных логических устройств. М.: Энергоатомиздат, 1986, 480 с.

32. Дружинин Г.В. Надежность автоматизированных производственных систем. М.: Энергоатомиздат, 1986, 480 с. 38. Зыль С.Н. Повышение отказоустойчивости сетевых приложений реального времени./ Сети и системы связи. 2005, №6. с 33 -37.

33. Дж. Уолренд Телекоммуникационные и компьютерные сети. М.: Постмаркет. 2001, 480 с.

34. Закон Российской Федерации "Об оперативно-розыскной деятельности в РФ", 1992.

35. Емелин Н.М., Новиков Н.Н., Павлов А.А. и др. Принцип агрегатно-модульной адаптации интеллектуальных систем к контролю технического состояния сложных объектов. // Измерительная техника. 1999, № 5. С. 43-46

36. Зайцев Г.В., Зиновьев В.А., Семаков Н.В. Коды с минимальной плотностью проверок для исправления байтовых ошибок, стираний, дефектов. // Проблемы передачи информации. 1983. Т. 19. № 3. С. 29-37

37. Защита от несанкционированного доступа к информации. Термины и определения. Руководящий документ Гостехкоммиссии России. М.: Военное издательство, 1992.

38. Зыль С.Н. Повышение отказоустойчивости сетевых приложений реального времени./ Сети и системы связи. 2005, №6. с 33 -37.

39. Иванов М.А., Кларин А.П. Сигнатурный анализ в задачах контроля и диагностики цифровых устройств. М.: Изд. МИФИ, 1986, 26 с.

40. Иуыду К.А. Надежность, контроль и диагностика вычислительных машин и систем. М.: Высшая школа, 1989, 215 с.

41. Каган Б.М., Мкртумян И.Б. Основы эксплуатации ЭВМ. М.: Энергоатомиздат, 1988, 430 с.

42. Казарин О.В., Лагутин В.С., Петраков А.В. Защита достоверных цифровых электрорадио сообщений. Учебное пособие.
-М,: РИО МГУ СИ, 1997. - 68 с.
43. Калинцев Ю.К. Криптозащита сообщений в системах связи. Учебное пособие.-М.: МТУСИ, 2000.- 236 с.
44. Обрайен Т., Подж С. Уайт Дж. Microsoft Access 97: разработка приложений: пер. с англ. - СПб.: БХВ - СПб., 1999. - 640 с.
45. Прокофьева Н.О.,Зайцева Л.В., Куплис У.Г. Компьютерные системы в дистанционном образовании // Телематика-2001: Труды междунар. науч.-метод. конф. СПб., 2001. С. 109-111.
46. Рогов С., Намиот Д. Тестирование производительности Web-серверов. Сибинфоцентр. http://www.sibinfo.ru/news/03_0 l_08/server_testing.shtm (17 июня 2003).
47. Российский портал открытого образования: обучение, опыт, организация/ Отв. ред. В.И. Солдаткин. - М.: МГИУ, 2003. - 508 с.
48 . Солдаткин. В.И. Информационно-образовательная среда открытого образования // Телематика-2002: Труды всерос. науч.-метод. конф. СПБ., 2002. с. 281-284.
49. Мырова Л.О., Попов В.Д. Анализ стойкости систем связи к воздействию излучений. М.: Радио и связь, 1993. С.21-28.
50. Мур М, Притск Т., Риггс К., Сауфвик П. и др. Телекоммуникации. СПб.: БХВ - Петербург, 2005. - 624 с.
51. http://bugtraq.ru/library/internals/admintrap.html
52. Олифер В.Г, Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. СПб. Питер, 2004– 864 с.
53. Пархоменко П.П. Основы технической диагностики. Кн. 1.-М.: Энергия, 1976. 464 с.
54. Павлов А.А. Повышение достоверности функционирования микропроцессорных средств измерительной техники. // Измерительная техник. 1999, №4. С. 28-33.

55. Павлов А.А. Повышение достоверности функционирования устройств памяти ЭВМ на основе использования корректирующих кодов с апостериорной коррекцией ошибок.// КомпьюЛог. 1998, № 5,6 (29,30) С. 6-9.

56. Павлов А.А., Кузнецов А.Н. Метод построения отказоустойчивых дискретных устройств на основе корректирующих кодов повышенной обнаруживающей способности. // КомпьюЛог. 1998, № 4(28) С. 49-51.

57. Павлов А.А., Павлов А.А. Концептуальные основы построения отказоустойчивых запоминающих устройств с апостериорной коррекцией ошибок. // КомпьюЛог. 1999, № 1(31) С. 34-37.

58. Павлов А.А., Гориш А.В., Милов Ю.Г. Метод защиты памяти ЭВМ на основе корректирующих кодов с апостериорной коррекцией ошибок // Экология, мониторинг и рациональное природопользование. Научн. тр. Вып. 302(11)-М.: МГУЛеса, 1999, С.259-264.

59. Петраков А.В. Основы практической защиты информации М.: Радио и связь, 1999.- 368 с.

60. Петров Б.М. Рассмотрение основных показателей радиационной стойкости, позволяющих анализировать безотказность микропроцессорных и компьютерных устройств при радиационном воздействии // Сборник докладов международной НТК “Актуальные проблемы анализа и обеспечения надежности и качества приборов, устройств и систем”, Пенза, 1998, С. 325-327.

67. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, изд.2-ое.1996, 380 с.

68. Поваляев Э.И., Щербаков Ю.И. Аппаратно-ориентированный метод решения системы уравнений двоичных кодов БЧХ для процедуры параллельной коррекции трехкратных ошибок. // Автоматика и вычислительная техника. 1987. № 3. С. 66-71.

69. Половко А.М. Основы теории надежности. М.: Наука, 1964, 356 с.

70. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы сети и телекоммуникации./Учебник для ВУЗов. М.; Финансы и статистика, 2003, 560 с.

71. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях,-М.:Радио и связь,1999.-328 с.

72.Руководство по поиску неисправностей в объединенных сетях Cusco Systems. М.: Издательский дом “Вильямс”, 2003, 1040 с.

73. Саголович Ю.Л. Кодовая защита оперативной памяти ЭВМ от ошибок.// Автоматика и телемеханика, 1991, № 5, С. 4-40.

74. Сапожников В.В., Сапожников В.В, Методы синтеза надежных автоматов. Л.:Энергия, 1980, 94 с.

75. Согомонян Е.С., Слабоков Е.В. Самопроверяемые устройства и отказоустойчивые системы. М.: Радио и связь, 1989, 207 с.

76. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Термины и определения. Руководящий документ Гостехкоммиссии России. М.: Военное издательство, 1992.

77. Самофалов К.Г., Корнейчук В.И., Городний А.В. Структурно-логические методы повышения надежности запоминающих устройств. М.: Машиностроение, 1976, 350 с.

78. Суворов А.Б. Телекоммуникационные системы, компьютерные сети и Интернет./Учебное пособие для вузов. М.: Феникс, 2007, 384 с.

79. Терминологический словарь «Бизнес-Безопасность-Телекоммуникации»- Учебное пособие / Составители А.А.Аржанов, Е.Г.Новикова, А.В.Петраков, С.В. Рабовский.- М.: РИО МТУСИ, 2000.- 304 с.

80.Толстяков В.С. Обнаружение и исправление ошибок в дискретных устройствах. М.: Советское радио,1972, 288 с.

81.Шеннон К. Работы по теории информации и кибернетике. -М.: ИИЛ, 1963.- 829 с.

82. Халяпин Д. Б., Ярочкин В. И. Основы защиты промышленной и коммерческой информации. Термины и определения. М.: ИПКИР, 1994, 231 с.

83. Хетагуров Я.А., Руднев Ю.Л. Повышение надежности цифровых устройств методами избыточного кодирования. М.: Энергия,1974, 370 с.

84. Хестер Н. Frontpage 2002 для Windows: Пер. С англ. - М.: ДМК Пресс, 2002. – 448с.

85. Хорев А.А. Способы и средства защиты информации.- М.: МО РФ,2001.-316с.

86. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие.М.:Гостехкомиссия РФ, 1998-320 с.

87. Щербаков Н.С. Самокорректирующееся дискретные устройства. М.: Машиностроение, 1975, 214 с.

88. Щербаков Н.С. Достоверность работы цифровых устройств. М.: Машиностроение, 1989, 224 с.

89. Яблонский С. В. Введение в дискретную математику. М.: Наука,1979, 272 с.

90. Aichelmann F. J.Jr. Local paging memory buffer forminimizing Concurrence of hard and soft data errors. // IBM Tech. Disclosure Bull. 1980.№ 11. P. 4931-4932.

91. Blaum M. Systematic unidirectional burst detecting codes. //IBM RJ 5662 (57161), May 1987.

92. Bose B. On systematic SEC/MUED code. // Proc. FTCS. June 1981.V.11 P. 265-267.

93. Bose B. Systematic unidirectional error - detecting codes. //IEEE Trans. Computere. Nov. 1985. V.c-34 P. 1026-1032.

94. Chen C.L. Error correcting codes with Byte Error detection capability //IEEE Trans. Cjmpputere. July 1983. V.c-32 p. 615-621.

95. Libson M. R., Harvey H.E. A general-purpose memory reliability simulation. // IBM J. Res. Develop. 1984/ v.28. P. 196-206.

96. Meyer J.F., Wei L. Influence of workload on error recovery in random access memories. // IEEE Trans. Comput. 1988. V.37.№4. P, 500-507.

97. Nrener R., Fujiwara E., Agarwal V.K. Low Overhead, High Coverage Built-in Self-Test PLA Desidn/FTCS-15. 1985. P. 37-41.

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

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

100. 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.

101. 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.

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

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

104. Дарахма Ислам. Повышение отказоустойчивости транспортного уровня вычислительных сетей путем реорганизации сквозной «точка-точка» множественной адресации/ ГалкинА.П., АльджарадатМ.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.

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

106. 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.

107. http://www.mtit.pna.ps/ar/index.php

108. http://www.pma.ps/ar-eg/home.aspx

109. http://www.pibbank.com/ar/

110.http://scholar.najah.edu/sites/default/files/all-thesis/the_credit_policy_in_the_palestinian_banks.pdf

## Список сокращений

WAN- Глобальная вычислительная сеть

АБС - автоматическая биллинговая система

АКС - аппаратура конфиденциальной связи

БД - база данных

БЗ - база знаний

ВТСС - вспомогательные технические средства и системы

ЗИ – защита информации

ЗМ - защитные мероприятия

ИКТ - информационные и коммуникационные технологии

ИП - информационные потоки

ИСППР - интеллектуальная система поддержки принятия решений

КИТС - корпоративная информационно-телекоммуникационная сеть

КПИ - коэффициент потерь информации

КС - корпоративные сети

КУ - канал утечки

ЛВС ( LAN) - локальная вычислительная сеть

НИС - нечеткая интеллектуальная система

НСД - несанкционированный доступ

ПИП - повторные информационные потоки

СА - сетевые аномалии

СЗИ - система защиты информации

СОА (IDS) - систем обнаружения атак или вторжений

СОД - систем обработки данных

СППР - система поддержки принятия решений

СУБД - систе́ма управле́ния ба́зами да́нных

ТКУИ - технический канал утечки информации

ТС - телекоммуникационная система

ЭМ - эффективность моделирования

ЭПр - эффективность проектирования

ЭС - экспертные системы

ISS - системы безопасности Интернета

NE - элемент сети

SUID - комплект идентификатор пользователя

TCP - Transmission Control Protocol

**Приложение.**

Опр: ***Нечетким логическим выводом*** (fuzzy logic inference) называется аппроксимация зависимости $Y = f(X_1,X_2…X_n)$ каждой выходной лингвистической переменной от входных лингвистических переменных и получение заключения в виде нечеткого множества, соответствующего текущим значениях входов, с использованием нечеткой базы знаний и нечетких операций. Основу нечеткого логического вывода составляет композиционное правило Заде[1].

В общем случае нечеткий вывод решения происходит за три (или четыре) шага:

1) Этап фаззификации. С помощью функций принадлежности всех термов входных лингвистических переменных (ЛП) и на основании задаваемых четких значений из универсов входных лингвистических переменных определяются степени уверенности в том, что выходная лингвистическая переменная принимает значение – конкретный терм. Эта степень уверенности есть ордината точки пересечения графика функции принадлежности терма и прямой x = четкое значение ЛП.

2) Этап непосредственного нечеткого вывода. На основании набора правил – нечеткой базы знаний – вычисляется значение истинности для предпосылки каждого правила на основании конкретных нечетких операций, соответствующих конъюнкции или дизъюнкции термов в левой части правил. В большинстве случаев это либо максимум, либо минимум из степеней уверенности термов, вычисленных на этапе фаззификации. которое применяется к заключению каждого правила. Используя один из способов построения нечеткой импликации, мы получим нечеткую переменную, соответствующую вычисленному значению степени уверенности в левой части правила и нечеткому множеству в правой части правила.

Обычно в качестве для вывода используется минимизация или правила продукции. При минимизирующем логическом выводе, выходная функция принадлежности ограничена сверху в соответствии с вычисленной степенью истинности посылки правила (нечеткое логическое И). В логическом выводе с использованием продукций, выходная функция принадлежности масштабируется с помощью вычисленной степенью истинности предпосылки правила.

3) Этап композиции (агрегации, аккумуляции). Все нечеткие множества, назначенные для каждого терма каждой выходной лингвистической переменной, объединяются вместе, и формируется единственное нечеткое множество - значение для каждой выводимой лингвистической переменной. Наконец снова, обычно используются функции MAX или SUM.

4) Этап дефаззификации (необязательный). Используется тогда, когда полезно преобразовывать нечеткий набор значений выводимых лингвистических переменных к точным значениям. Имеется достаточно большое количество методов перехода к точным значениям. Два из общих методов - это «методы полной интерпретации» и «по максимуму». В методе полной интерпретации, точное значение выводимой переменной вычисляется как значение "центра тяжести" функции принадлежности для нечеткого значения. В методе максимума, в качестве точного значения выводимой переменной принимается максимальное значение функции принадлежности.

Главным же недостатком продукционных систем остается то, что для их функционирования требуется наличие полной информации о системе.

Нечеткие системы управления основаны на правилах продукционного типа, однако в качестве посылки и заключения в правиле используются лингвистические переменные, что позволяет избежать ограничений, присущих классическим продукционным правилам. В основу функционирования нечетких систем управления положен механизм нечеткого вывода, который рассматривается подробно в соответствующей главе работы. Результат нечеткого логического вывода является нечетким, а физическое исполнительное устройство не способно воспринять такую команду. Необходимы специальные математические методы, позволяющие переходить от нечетких значений величин к вполне определенным. Основные из этих математических методов.

**Логико-лингвистической модели**

Следует отметить тот факт, что с помощью преобразований нечётких множеств любое правило содержащее в левой части как конъюнкции, так и дизъюнкции можно привести к системе правил, в левой части каждого будут либо только конъюнкции, либо только дизъюнкции. Таким образом, не уменьшая общности, можно рассматривать правила, содержащие в левой части либо только конъюнкции, либо только дизъюнкции.

Каждое из правил представляет себя нечёткую импликацию. Степень уверенности посылки мы вычислили, а степень уверенности заключения задаётся функцией принадлежности соответствующего терма. Поэтому, используя один из способов построения нечёткой импликации мы получим новую нечёткую переменную, соответствующую степени уверенности о значении выходного значения при применении к заданным входным соответствующего правила.

Теперь необходимо объединить результаты применения всех правил. Этот этап называется аккумуляцией. Один из основных способов аккумуляции – построение максимума полученных функций принадлежности. Получаем:

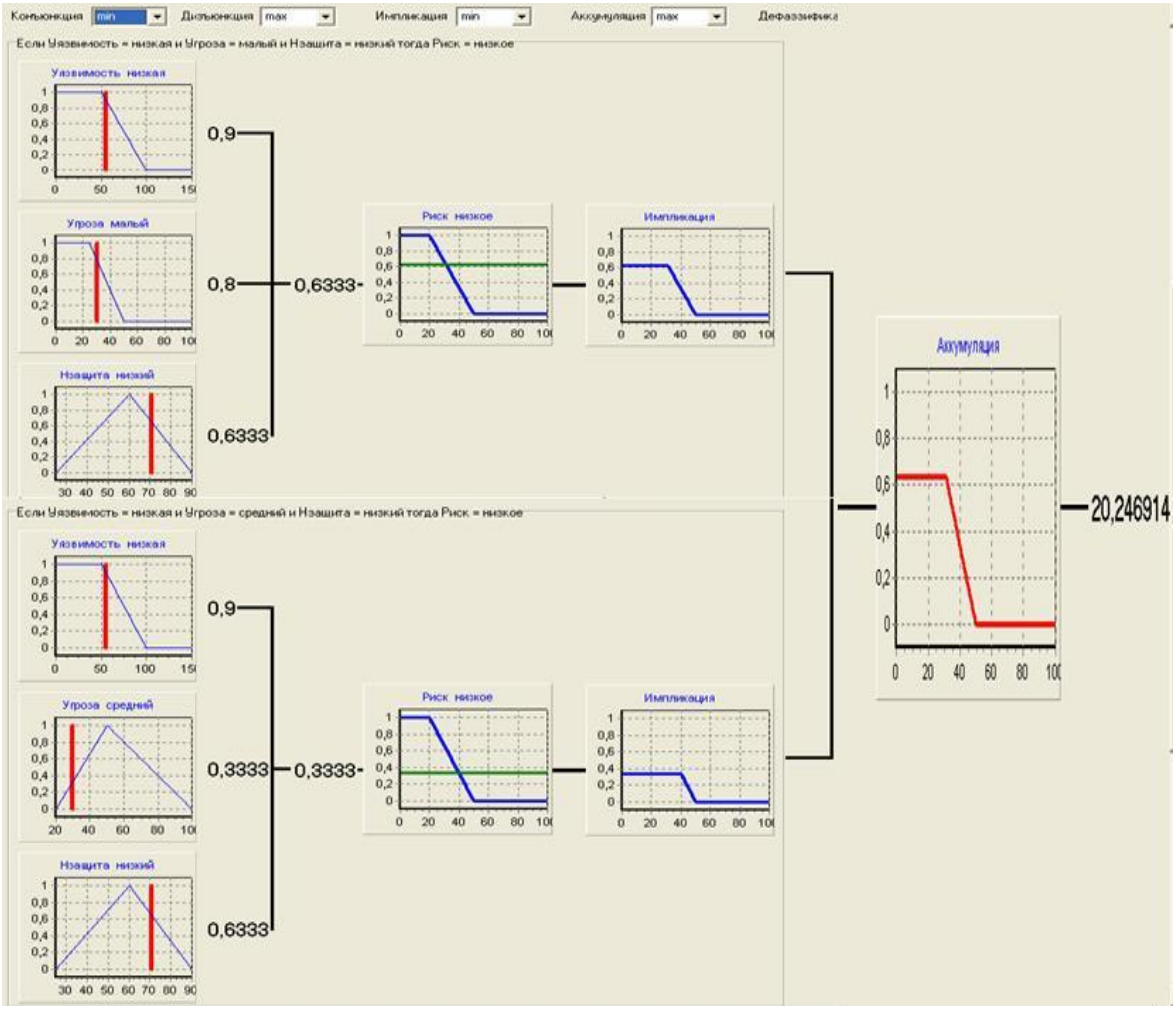



Рис 1. Нечёткий вывод

Полученную функцию принадлежности уже можно считать результатом. Это новый терм выходной переменно риск. Его функция принадлежности говорит о степени уверенности в значении риск при заданных значениях входных параметров и правилах, определяющих соотношение входных и выходных переменных. Но обычно всё-таки необходимо, какое то конкретное числовое значение. Для его получения используется этап дефаззификации, т.е. получения конкретного значения из универса по заданной на нём функции принадлежности.

Существует множество методов дефаззификации, но в нашем случае достаточно метода первого максимума. Применяя его к полученной функции принадлежности, получаем, что значение уверенность риска 20,245914.

Посольство
Государства Палестина в
Российской Федерации

سفارة دولة فلسطين
لدى
روسيا الإتحادية

Ref : №1663

Date : 26/11-2014г.

ФГБОУ ВПО «Владимирский государственный
университет имени Александра Григорьевича и
Николая Григорьевича Столетовых» (ВлГУ)
Зав. кафедрой радиотехники и радиосистем
Заслуженному деятелю науки РФ, д.т.н., проф. О.Р. НИКИТИНУ

Многоуважаемый Олег Рафаилович!

Мы искренне рады, что Ваша кафедра успешно участвует в подготовке профессиональных специалистов, включая уроженцев Палестины, которые очень нужны нашей родине. Высочайший уровень обучения молодёжи на Вашей кафедре хорошо известен в Палестине.

В настоящее время для нас важно и актуально выполнить ряд работ по информационной защите телекоммуникационных сетей для применения в разных областях, в том числе и в национальных банковских сетях с учетом особенностей нашей страны.

Правительство Палестины поручило аспиранту Дарахма Исламу изучить и подготовить диссертационную работу по теме: «Защита банковских компьютерных сетей от несанкционированного доступа в Государстве Палестина». Результате данной работы после её защиты обязательно будут внедрены в соответствующей сфере в нашей стране. Для нас важно, чтобы в работе были использованы элементы нечеткой логики и MAT LAB, так как эти математические подходы популярны в Палестине и будут поняти и приняты нашими специалистами.

Просим оказать аспиранту Дарахма Исламу всестороннюю поддержку для завершения его значимой работы и, по возможности, помочь ему внедрить разработки в России в подобных по сетевой структуре палестинским предприятиям.

Выражаем огромную благодарность лично Вам и Вашему великолепному коллективу и надеемся на дальнейшее многолетнее сотрудничество с Вами, с Вашим университетом в благородном деле подготовки высококвалифицированных специалистов.

ШАМСЕДДИН БАДРАН
Первый Секретарь Посольства
Государства Палестина в Российской Федерации

119034 Москва, Кропоткинский пер, 26 119034 Moscow, Kropotkinsky per, 26
Tel: +7-495-6374340, 6373682, Fax: +7-495-6372195
E-mail: embassy@palestine.ru Website:www.palestine.ru

**«Утверждаю»**

**Генеральный директор**

**ПФ «Электроприбор»** (г. Москва)

**Н. И. Захарова**

4 ноября 2014 г.

## Акт внедрения

Результаты, полученные Дарахма Исламом (гражданином Палестины) при выполнении диссертационной работы, внедрены на нашем предприятии в 2013-14 гг. в виде расчетных методик и алгоритмов, в частности, с учетом экономической целесообразности защиты информации.

Особенно интересным для нас оказалось применение элементов нечеткой логики и методик оценок эффектов от этого. Высокий уровень подтверждается применением солидного математического аппарата и другими разработками.

Проведена проверка на наличие возможных путей проникновения в информационные сети нашего предприятия и защиты от них.

Использованы рекомендации по защите компьютерных и телекоммуникационных сетей от несанкционированного доступа к информации применительно к нашему предприятию.

Начальник информационного отдела - **Иванов А.П.**

Администратор сети - **Володин А.И.**

**«Утверждаю»**
**Генеральный директор**
**НПО «РИК»,** г. Владимир

**к. т. н.-**

**А. В. Поляков**
27.10.14

## Акт внедрения

Результаты, полученные **Дарахма Исламом** (гражданин Палестины) при выполнении диссертационной работы, в частности:

1) Методики применения различных способов защиты информации от несанкционированного доступа и оценки эффективности этого;

2) Рекомендации по защите телекоммуникационных и компьютерных сетей;

3) Использование элементов нечеткой логики для информационной защиты и анализ эффекта от этого;

внедрены на нашем предприятии в 2012-2014гг. Они нашли практическое применение при обмене информацией с нашими филиалами в гг. Иваново, Санкт-Петербург, Омск и т.п.

Указанные методики хороши тем, что при сравнительно небольших затратах на оборудование и программное обеспечение обеспечивают высокую эффективность и не требуют специальной подготовки нашего персонала.

Начальник отдела- Сирко С. Э.

Начальник лаборатории - Смушко О.Л.