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)

На правах рукописи

**Альджарадат Махран Мохаммад Али**

# ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОБРАЗОВАТЕЛЬНЫХ СЕТЯХ ПАЛЕСТИНЫ

Специальность: 05.12.13 – «Системы, сети и устройства телекоммуникаций»

**Диссертация на соискание ученой степени**

кандидата технических наук

Научный руководитель:

доктор технических наук,

профессор Галкин А.П.

Владимир 2014

**СОДЕРЖАНИЕ**

## СПИСОК СОКРАЩЕНИЙ

АКС - аппаратура конфиденциальной связи

АНБ - Агентство национальной безопасности (США)

АШКУ - абонентское шифрующее и кодирующее устройство

БД - база данных

БЗ - база знаний

БС - базовая станция

ВТСС - вспомогательные технические средства и системы

ДО - дистанционное обучение

ЗАС - аппаратура засекречивания

ЗМ - защитные мероприятия

КЗ - контролируемая зона

КИТС – корпоративная информационно-телекоммуникационная сеть

КП - коммутация пакетов

КПИ - коэффициент потерь информации

КС - канал связи

ЛВС - локальная вычислительная сеть

НСД - несанкционированный доступ

ОЗУ - оперативное запоминающее устройство

ПИП - повторные информационные потоки

ПК - персональный компьютер

РЭС - радиоэлектронные средства (радиоэлектронная система)

СДО - система дистанционного обучения

ТКУИ - технический канал утечки информации

ТС - телекоммуникационная система

ТСПИ - технические средства приема, обработки, хранения и передачи информации

ТСР - технические средства разведки

ШУ - шифрующее устройство

ЭМ - эффективность моделирования

ЭПр - эффективность проектирования

# ВВЕДЕНИЕ

## Актуальность проблемы

Сейчас компьютеры действительно стали приобретать качества, позволяющие называть их интегральными устройствами обработки информации и телекоммуникаций, появилась возможность реально их использовать результаты этих достижений и для цели систем дистанционного образования (СДО). Это характерно для всех арабских стран, в которых наблюдается тенденция стремительного развития цифровых технологий, вызванная интенсивным внедрением компьютерных телекоммуникационных сетей (ТС)[1, 2, 4, 16, 53, 63, 74,75].

Аналогичные проблемы, задачи и трудности есть и в Палестине. Они усугубляются еще и становлением в ней информационных технологий и телекоммуникаций, несколько запоздалым по различным причинам [107, 108].

Использование таких средств не является самоцелью, а лишь средством интенсификации каналов связи. Что крайне важно для СДО. Попытки достичь этой цели предпринимаются с момента появления массовой корпоративной связи.

Сильную популярность современные виды телекоммуникаций, в том числе и для целей СДО приобрели в странах, характеризующихся:

-значительными территориями;

-невысоким уровнем жизни;

-неустойчивым экономическим положением;

-наличием непомерно высокого спроса на обычные телекоммуникации.

Абсолютное большинство этих факторов конкретно относятся к современной Палестине [107, 108].

В Палестине внедрения технологий на основе компьютерных телекоммуникаций, могут вызвать существенные трудности и помехи [52], среди которых (табл.1.1.1).

Таблица 1.1.1.Трудности Палестинских СДО

| Особенности, трудности | Направление решения |
|---|---|
| ненасыщенный и устаревший, структурный состав оборудования учреждений и у многих индивидуальных пользователей | Обеспечение ПК и ТС |
| слабое развитие компьютерных ТС СДО, их нестабильность | оснащение |
| недостаточная подготовка сетевых администраторов | обучение |
| языковые трудности | переподготовка |
| неудовлетворительная компьютерная грамотность населения, что создает дополнительные психологические барьеры в развитии телекоммуникаций | обучение |
| подавляющая часть ПК и ТС не удовлетворяет критериям, предъявляемым к ним с точки зрения защиты от несанкционированного доступа (НСД) к информации[67] | оснащение |
| адаптировать возможности приобретаемого продукта для особенностей Палестины | Оснащение, обучение |

Для информационного обеспечения процессов телекоммуникационного обмена используются многие факторы[18, 25, 45, 65], которая может быть эффективно реализована только в условиях качественных каналов связи.

Это условие выполняется еще далеко не во всех районах Палестины [107,108]. Необходима разработка информационно-программных сред, учитывающих требования современных предприятий Палестины и, в частности, СДО, а также особенности состояния сетевых коммуникаций в наших регионах очень важно.

Надо информационно защищать предприятия и учреждения образования Палестины для обеспечения их учебной конкурентоспособности во всех сферах, а в СДО особенно, а именно в ТС.

**Объект исследования** – системы корпоративных телекоммуникаций СДО Палестины и защита их от несанкционированного доступа к информации.

**Цель работы** - решение научно-технических задач, связанных с созданием комплекса методик для повышения помехозащищенности связи и разработкой методов и средств по обеспечению информационной безопасности СДО Палестины и, следовательно, для повышения уровня конкурентоспособности. Для достижения указанной цели в диссертации сформулированы и решены следующие **научные и технические задачи**:

- анализ защищенных информационных сред в ТС СДО;

-оценка и предъявление конкретных требований к структуре телекоммуникационных сетей и функциональным возможностям отдельных ее частей;

-разработка программного обеспечения (ПО) для выполнения администрирования;

-разработка и проведение оценки показателей надежности, и уровня технического состояния защищаемого канала;

-выработка принципов, алгоритмов и методик поиска технических устройств НСД к информации, которые могут быть реализованы при ограниченных возможностях СДО учебных заведений Палестины;

- разработка критериев оценки эффективности информационного канала с учетом защитных мероприятий;

-разработка разнообразных методик обоснования мероприятий по защите от несанкционированного доступа;

- разработка методик и алгоритмов синтеза защищенных сетей с роутерами;

- разработка эффективных компьютерных программ для поиска проникновений в телекоммуникации.

**Методы исследования.** При решении поставленных задач использован аппарат математического анализа, теории вероятностей, теории надежности и программирования.

Основные теоретические результаты проверены в конкретных системах и с помощью программ на ПК и в ходе испытаний, эксплуатации и внедрения в СДО в Палестинском политехническом университете и в КИТС и в реальных сетях СДО.

**Научная новизна работы** заключается в следующем:

1. Проведен анализ и систематизация существующих программных продуктов, выполняющих функции информационных сред;
2. Исследована и оценена целесообразность проведения защитных мероприятий для конкретных предприятий и учебных заведений для целей повышения их эффективности с учетом особенностей Палестины;
3. На основе теорий надежности разработаны методики защиты информации в современной системе связи для целей СДО;
4. Проведены практические исследования предложенных схем защиты информации в корпоративных системах связи, аналогичных по свойствам СДО.

**Практическая ценность работы**.

1. Разработанные методики и программные средства могут быть использованы в телекоммуникационных сетях конкретных предприятий. При этом:
2. Проведены исследования по выбору оснащения для определенных, конкретных СДО Палестины;
4. Определены требования к современной КИТС СДО и защищенной информации с помощью разработанных методик;

5. Выбор средств и структур защищенной СДО и КИТС обеспечили несколько методик;

6. Разработаны подходы к поиску проникновений в СДО, обеспечение высоких эффективности и конкурентоспособности;

7. Разработаны принципы построения системы защиты информации в современных СДО, которые позволили сократить время проектирования в 3 раза, а число маршрутизаторов в 2 раза;

8. Созданы методики определения заданной целесообразности защиты информации в СДО и эксплуатационной надежности в смысле проникновений;

9. Найдены подходы для поиска проникновений в СДО и КИТС с эффективной защитой образовательной информации;

10. Программные продукты и методики по защите информации в каналах СДО реализованы в ППУ- Палестинском политехническом университете и на ряде предприятий России и показали свою жизнеспособность и эффективность и удовольствие заказчиков.

Акты внедрения результатов диссертационной работы представлены в ПРИЛОЖЕНИИ.

**Достоверность полученных результатов** в диссертации подтверждается использованием расчетных методик, разработанных автором, на основе аппарата теории вероятностей и случайных процессов, теории надежности, теории нелинейных динамических систем, вычислительной математики и программирования.

В диссертации использованы результаты исследований и разработокдля защиты СДО Палестины от несанкционированного доступа к информации с оценкой их эффективности по критериям и методикам, предложенных автором, которые получили всемерное одобрение на родине автора.

**Результаты внедрения работы.** Основные теоретические и практические результаты получены автором при выполнении диссертационной работы, были внедрены в ППУ «Палестинском политехническом университете», (Палестина), в корпоративной сети завода «Электроприбор» (г. Москва) при повышении уровня информационной безопасности сети; в НПО «РИК» (Ремонт инженерных конструкции) г. Владимир.

**Апробация работы.** Основные научные и практические результаты работы докладывались и обсуждались на 5-ти международных конференциях, в том числе: на международных научно технической конференции «Перспективные технологии в средствах передачи информации», г. Владимир, 2013г.; Международной научной конференции «Физика и радиоэлектроника в медицине и экологии», г. Владимир-Суздаль, 2012,2014 г.; Межрегиональной научной конференции «Инновационное развитие экономики – основа устойчивого развития территориального комплекса», Институт экономики АН РФ, г. Владимир - г. Москва, 2012 г.; Международной научной конференции «Урбанистика городов с историческим ядром», г. Владимир 2012 г.; Международной научной конференции «Институт экономики АН РФ», Второй Российский экономический конгресс г. Суздаль - г. Владимир, 2013г.

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

**Структура и объём диссертации.**

Диссертация состоит из введения, четырёх глав, заключения, списка использованной литературы, включающего 108 наименований, списка

сокращений и 2 приложения. Объём диссертации: 134 страницы текста, 28 рисунков и 22 таблицы.

# ГЛАВА 1. СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ (СДО) ПАЛЕСТИНЫ И НЕОБХОДИМОСТЬ ЗАЩИТЫ ИХ ТЕЛЕКОММУНИКАЦИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

## 1.1. Информационные технологии в сетях Палестины

С получением относительной самостоятельности, в Палестине насущно встал вопрос об организации СДО. Поэтому диссертационная работа делается по заказу правительства Палестины.

В большинстве арабских стран произошло насыщение радиочастот. Но одновременно, в результате создания в 1967 г. Арабской организации по спутниковому вещанию (Arab Satellite Communications Organisation, ARABSAT) были созданы условия для расширения каналов телевещания и телефонной связи и, в том числе и для СДО.

Первый арабский спутник связи был запущен в 1985 г. Свободные каналы были использованы министерствами информации арабских стран (для нужд телерадиовещания), а также министерствами связи совместно с наземными службами. Действуя в качестве коммерческой организации, ARABSAT смог последовательно профинансировать все свои проекты. На его средства были созданы три спутника первого поколения, закуплены два уже действующих спутника с целью удовлетворения растущего спроса, а также запущены два спутника второго поколения для расширения действующей инфраструктуры. Первый спутник третьего поколения был запущен 27 фев. 1999 г. и обслуживает арабский регион, особенно в Палестине и стран Европы (табл.1.1.2).

Применяемость различных подходов в СДО Палестины приведена в табл.1.1.3.

Таблица 1.1.2. Отличительные черты внутреннего и внешнего оснащения СДО Палестины

| Элемент | Внутренний | Внешний |
|---|---|---|
| Объект | Определяются руководством | Определяются договором |
| Квалификация персонала | Определяется администрацией, свобода действий ограничена | Представляются жесткие требования со стороны профессиональных организаций. Большая степень свободы |
| Методы | Имеется большое сходство в используемых методах. Различия существуют в степени детализации проверок и в при контроле поступлений денежных средств | |
| Цели | Определяются руководством либо явным образом, либо вытекают из планов | Проистекают из законоположений документов судебных инстанций, а также из внешних потребностей |
| Отчетность | Перед руководством | Перед третьими лицами |

Таблица 1.1.3. Решение вопросов и проблем СДО в Палестине

| Подходы к СДО Палестины | обеспечение |
|---|---|
| Сети передачи данных общего пользования переходят со стандарта X.25 на стандарт Frame Relay, FR, и асинхронную передачу данных (ATM) | Правительство |
| Подключение к Интернету осуществляется различными способами: через спутник либо при помощи волоконно-оптического кабеля. Общая пропускная способность каналов подключения к Интернет достигла 12 Мбит/с., из | Правительство |

| | |
|---|---|
| которых 2,5 Мбит/с. приходятся на сеть Палестинских университетов (Palestine Universities Network) | |
| Некоторые удаленные от северной части Палестины провайдеры для местной связи используют терминалы с очень малой апертурой (VSAT) | |
| Академия наук и технологий всячески способствует доступу к базам данных научных библиотек и патентной информации. Информационная сеть Палестинских университетов выполняет роль общенациональной административной службы, а Центр информации и поддержки принятия решений (Information and Decision Support Centre) контролирует предоставление Интернет-услуг госучреждениям и предоставляет лицензии частным сервис-провайдерам. | Правительство |
| внедрение компьютеров в университетах с целью обучения учащихся, преподавателей и администрации основам ИТ | Правительство, Министерство образования |
| применение компьютеров в сочетании с мультимедийными устройствами для оказания помощи в преподавании различных предметов, опробования новых методов обучения и закрепления знаний | Министерство образования, университеты |
| использование Интернет для укрепления связей между арабскими учащимися и их сверстниками по всему миру и экспериментального обучения с помощью Web | Правительство, университеты |
| подготовка преподавателей и поддержка административных работников системы образования путем проведения видеоконференций | Министерство образования, университеты |

Палестина, в особенности СДО включила ИТ в список основных приоритетов развития и рассматривает их в качестве основного элемента образования, связи и научного обмена. Необходима работа по дальнейшей

систематизации стратегических планов с целью развития интегрированных информационных систем, способных оказать многоуровневую поддержку расширяющемуся сотрудничеству между предприятиями в рамках целой страны. В том, что касается повышения эффективности и действенности, качество самой информации, ее поиск и наличие организаций, занимающихся ее сбором и подтверждением, являются залогом достижения положительных результатов.

Для реализации услуг и механизмов защиты или управления защищенной системой в образовательных сетях СДО используются такие компоненты, как компонент управления средствами идентификации и аутентификации; компонент обеспечения целостности и конфиденциальности; компоненты управления средствами защиты базового программного обеспечения (при их наличии); компоненты управления средствами защиты прикладного программного обеспечения; компонент управления средствами контроля физического доступа (рис. 1.1.1.) .

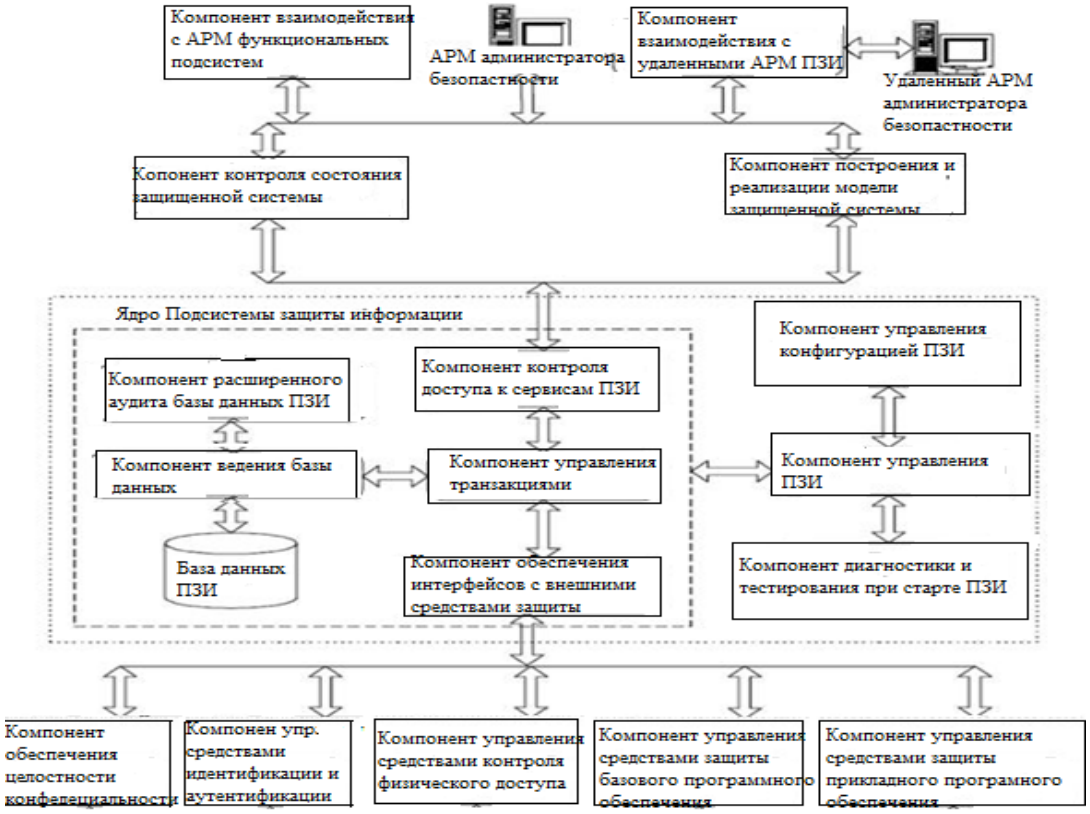



Рис.1.1.1. Структура подсистем защиты информации в Палестине

## 1.2. Классификация СДО Палестины

### 1.2.1. Основные направления и проблемы в СДО Палестины

С получением относительной самостоятельности, в Палестине насущно встал вопрос об организации СДО. Эта работа делается по заказу правительства Палестины. Мы используем опыт арабских стран в этих вопросах и, в частности, внедренную в Палестине, диссертацию Аль-Агбари [14], выполненную под руководством Галкина А.П.

Проблема дистанционного обучения особенно актуальна для Палестины как и для Палестины из-за неразвитости инфраструктуры и из-за плохой информационной защищенности[107,108].

Под дистанционным обучением следует понимать образовательную систему на основе компьютерных телекоммуникаций с использованием современных педагогических и информационных технологий [14-20].

СДО в Палестине это комплекс, обеспечивающий получение образования от начального до высшего.

К первому направлению можно отнести расширение доступности образования.

Ко второму типу - относится изменение качества образования: усиление роли самостоятельного обучения, освоение новых информационных технологий, использование дополнительных образовательных ресурсов (табл.1.2.1.1).

Таблица 1.2.1.1.Деятельность по развитию СДО Палестины

| Развитие образования | Учет СДО |
|---|---|
| 1. Планирование | 1. Установление стандартов, вычисление возможных знаменателей. |
| 2. Принятие решения | 2. Сбор соответствующих стоимостных и прочих пояснений; представление и использование их в знаменателях; предложение указаний для выбранного знаменателя |
| 3. Контроль (тождество с планом) | 3. Сближение практических результатов с нацеленными в планах и балансе, разъяснение отклонений как положительных, так и отрицательных |

В качестве основы дистанционного обучения целесообразнее всего использовать компьютерные телекоммуникации [22,23], которые предоставляют (табл. 1.2.1.2.):

Таблица 1.2.1.2. Направления СДО в Палестине

| Возможности | обеспечение |
|---|---|
| оперативной передачи на любые расстояния информации любого объема и вида | Операторы, сети СДО |
| интерактивность и оперативность обратной связи | Интернет |
| доступ к различным источникам информации (в том числе и использование развитой структуры на арабском языке) | Операторы, сети СДО |
| организации совместных телекоммуникационных проектов | Операторы, сети СДО |
| запрос информации по любому интересующему вопросу через электронные конференции | Интернет, сети СДО, партнеры |

Все эти возможности естественно осуществимы только в защищенных сетях[14,74,75,90,93-97]. В системах дистанционного образования существует четкая иерархия пользователей.

Администратор системы следит за всей системой дистанционного образования и обычно имеет доступ ко всем данным сформированным СДО[24], а именно, с разновидностью заочного обучения, только с использованием компьютерных телекоммуникаций[14].

Схема СДО создает структуру, которая показана на рис.1.2.1.
Она безусловно сильно упрощена по сравнению с реальностью, но дает очень хорошее представление о сути процессов в СДО Палестины.

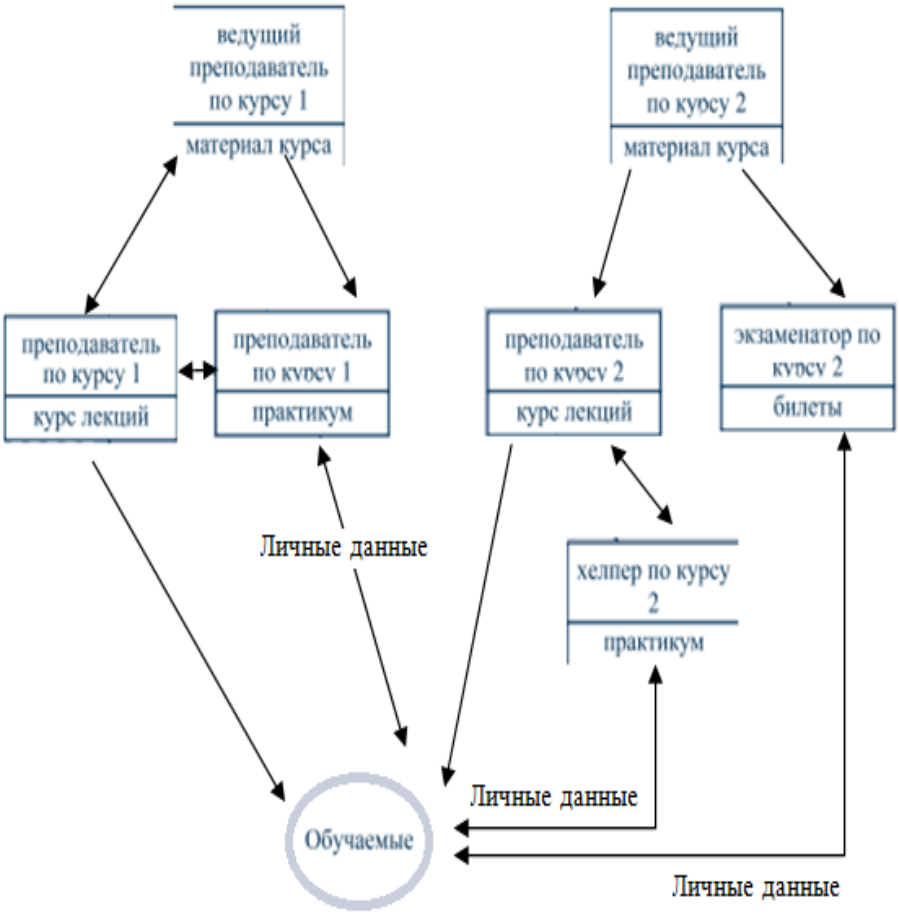



Рис.1.2.1. Упрощенная схема пользователей системы дистанционного образования

Существующие СДО можно разделить на несколько групп, в соответствии с предоставляемыми возможностями[14]:

Проведение учебных курсов обходится затратно, с большой нагрузкой на бюджет, поскольку они требуют информационной защиты[14].

Расчет основного капитала или инвестиций в сектор СДО, представленные в создании главного капитала, подобно приросту постоянного, нового или основного капитала, и положительные изменения товарных запасов и выполняемых проектов, подобно тому, как поясняется источник финансирования этих инвестиций, доходы

этого сектора и источники самофинансирования, резервы, заказанные ассигнования и кредит. Приведем структурный состав предполагаемого рынка СДО (табл.1.2.1.3)

Таблица 1.1.7**.** Количество обучающихся в государственных и частных университетах

| Года | 2012/2013 уч. г. | | 2013/2014 уч. г. | |
|---|---|---|---|---|
| Университеты | Кол-во фак-в | Кол-во студентов | Кол-во фак-в | Кол-во студентов |
| Госуд. | 5 | 21304 | 5 | 22580 |
| Частн. | 5 | 1668 | 6 | 3536 |
| Общ. | 10 | 22972 | 11 | 26116 |

В Палестине в СДО есть специальные компьютерные программы, для экзаменации пользователя (тьютора, студента), для электронных библиотек[107,108].

## 1.3. Риски в телекоммуникациях и критерии оценки защищенности от несанкционированного доступа

### 1.3.1. Риски и инвестиции в информационную безопасность СДО

Инвестиции в информационную безопасность СДО могут рассматриваться как инвестиции для увеличения эффективности путем уменьшения административных затрат на ее поддержание или для защиты от потерей путем предотвращения потенциальных затрат в случае негативных последствий [25-27,74]. В любом случае стоимость средств обеспечения безопасности должна соответствовать риску и прибыли для той среды, в которой используется данная СДО (см. табл.1.3.1.1).

Таблица 1.3.1.1. Основные показатели занятости Палестины 2005 – 2013 г.г.

| Показатель | 2005 | 2007 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|
| Всего предпр. | 33832 | 34181 | – | 37595 | 42116 | 42116 | 42116 |
| Кол-во малых предприятий (1-4 работника) | 32139 | 32480 | – | 34383 | 37334 | 37334 | 37334 |
| Кол-во средних предприятий (5-9 работников) | 1316 | 1323 | – | 2661 | 3686 | 3686 | 3686 |
| Кол-во крупных предприятий (10 и более работников) | 377 | 378 | – | 551 | 1096 | 1096 | 1096 |
| Общее кол-во работников | 113491 | 115760 | 128816 | 136734 | 188936 | 202871 | 254453 |

Оценка рисков информационной безопасности состоит из трех основных этапов: идентификация угроз, идентификация уязвимостей, идентификация активов (рис. 1.3.1.1)

Рис.1.3.1.1 Безопасность СДО Палестины

Многое определяется политикой защиты, которая зависит от (табл.1.3.1.2):

Таблица 1.3.1.2. Политика СДО

| Угрозы, уязвимости, политика | обеспечение |
|---|---|
| Уровня угроз, которым подвергается СДО и видимость СДО из внешнего мира | Проект, заказчик |
| Уязвимости СДО к последствиям потенциальных инцидентов с безопасностью | Проект, заказчик |
| Государственные законы и требований руководящих документов, которые могут явно определять необходимость проведения того или иного вида анализа риска или диктовать применение конкретных средств обеспечения безопасности для конкретных объектов, модулей или приложений (к сожалению, в Палестине, по этим вопросам, правовая вооруженность еще недостаточна!) | Проект, администрация |

### 1.3.2. Угрозы безопасности в СДО Палестины

Все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса.

Угроза - это любое событие, которое потенциально может нанести вред путем раскрытия, модификации или разрушения информации, или отказа в обслуживании критическими сервисами[14].


Рис.1.3.2.1. КИТС и безопасность в СДО Палестины

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

Типичные сетевые и телекоммуникационные угрозы [36-40] приводим сокращенно в табл.1.3.2.1:

Таблица 1.3.2.1. Типичные сетевые и телекоммуникационные угрозы

| Угрозы | В чем заключается | Кто страдает |
|---|---|---|
| Сбой в работе одной из | Срыв в обслуживании или | Тьюторы, |

| | | |
|---|---|---|
| компонент телекоммуникационной сети из-за ошибок при проектировании или отказов оборудования или программ | компрометации безопасности из-за неправильного функционирования одной из компонент телекоммуникационной сети. | студенты |
| Сканирование информации - неавторизованный просмотр критической информации злоумышленниками или авторизованными пользователями | Электронное письмо с неверным адресатом, распечатка принтера, неправильно сконфигурированные списки управления доступом, совместное использование несколькими людьми одного идентификатора и т.д. | Тьюторы, студенты, администрация, партнеры |
| Использование информации не по назначению - использование информации для целей, отличных от авторизованных | К отказу в обслуживании, излишним затратам, потере репутации. Виновниками этого могут быть как внутренние, так и внешние пользователи | Администрация, партнеры |
| Неавторизованное удаление, модификация или раскрытие информации - специальное искажение информационных | Потеря целостности или конфиденциальности информации | Тьюторы, студенты, администрация, партнеры |

| | | |
|---|---|---|
| ценностей | | |
| Проникновение - атака неавторизованных людей или систем, несанкционированное изменение параметров телекоммуникационной сети | Отказ в обслуживании или значительные затраты на восстановление после инцидента | Администрация, партнеры |
| Маскарад - попытки замаскироваться под авторизованного пользователя для кражи сервисов или информации, или для инициации финансовых транзакций | Финансовые потери или проблемы для СДО. | Тьюторы, студенты, администрация, партнеры |

Анализируя табл.1.3.2.1 можем сделать заключение, на основе опыта Аль-Агбари [14] , а также, нашего опыта и наших внедрений: наличие угрозы необязательно означает, что она нанесет вред.

### 1.3.3. Основные известные возможности информационной защиты СДО

По сложившемуся мнению экспертов в политике защиты должны быть рассмотрены, по крайней мере, следующие аспекты [53,75], которые мы сведем в табл. 1.3.3.1:

Таблица 1.3.3.1. Политика сетевой защиты в СДО Палестины

| Сетевые возможности | Кто обеспечивает |
|---|---|
| безопасность телекоммуникационных сетей | администрация, администраторы сети |

| | |
|---|---|
| санкционирование доступа к компьютерным системам, идентификация и аутентификация пользователя | администрация, администраторы сети |
| контроль прав доступа | Тьюторы, администраторы сети |
| мониторинг защиты и анализ статистики | администраторы сети, администрация, |
| конфигурирование и тестирование систем | администраторы сети |
| обучение мерам безопасности | Тьюторы, администраторы сети |
| физическая безопасность | администрация, охрана |

Центральная роль в современных системах безопасности возлагается на процедуры идентификации и аутентификации [14,54 ,55].

Существует три основных вида аутентификации - статическая, устойчивая и постоянная (табл.1.3.3.2).

Таблица 1.3.3.2. Виды аутентификации

| Виды | обеспечение |
|---|---|
| Статическая аутентификация использует пароли и другие технологии, которые могут быть скомпрометированы с помощью повтора этой информации атакующим. Часто эти пароли называются повторно используемыми паролями. | администраторы сети |
| Устойчивая аутентификация использует криптографию [56-62] или другие способы для создания одноразовых паролей, которые используются при проведении сеансов работы. Этот способ может быть скомпрометирован с помощью вставки сообщений атакующим в соединение. | администраторы сети, тьюторы |

| | |
|---|---|
| Постоянная аутентификация предохраняет от вставки сообщений атакующим | администраторы сети, проект |

Использование паролей в СДО Палестины обеспечивают такой вид защиты, но сила аутентификации зависит от сложности паролей и как они защищены. Одноразовые пароли и электронные подписи могут обеспечить хороший уровень защиты[14].

Известны три базовых способа их реализации, которые мы сведем в табл.1.3.2.4 и покажем на рис.1.3.3.1.

Таблица 1.3.2.4. Базовые способы криптографии

| Принцип | Кто владеет | Кто обеспечивает |
|---|---|---|
| с помощью известного пользователю пароля или условной фразы | Тьюторы, студенты, администрация, партнеры, администраторы сети | администрация, администраторы сети |
| С помощью персонального устройства/документа, которым владеет только пользователь: смарт-карты, карманного аутентификатора или просто специально изготовленного удостоверения личности (предполагается, что аутентитификатор никогда | Тьюторы, студенты, администрация, партнеры | администраторы сети |

| | | |
|---|---|---|
| никому не будет передаваться) | | |
| через аутентификацию самого пользователя - по отпечаткам пальцев, голосу, рисунку сетчатки глаза и т.п. | Тьюторы, студенты, администрация, партнеры | администрация, администраторы сети |

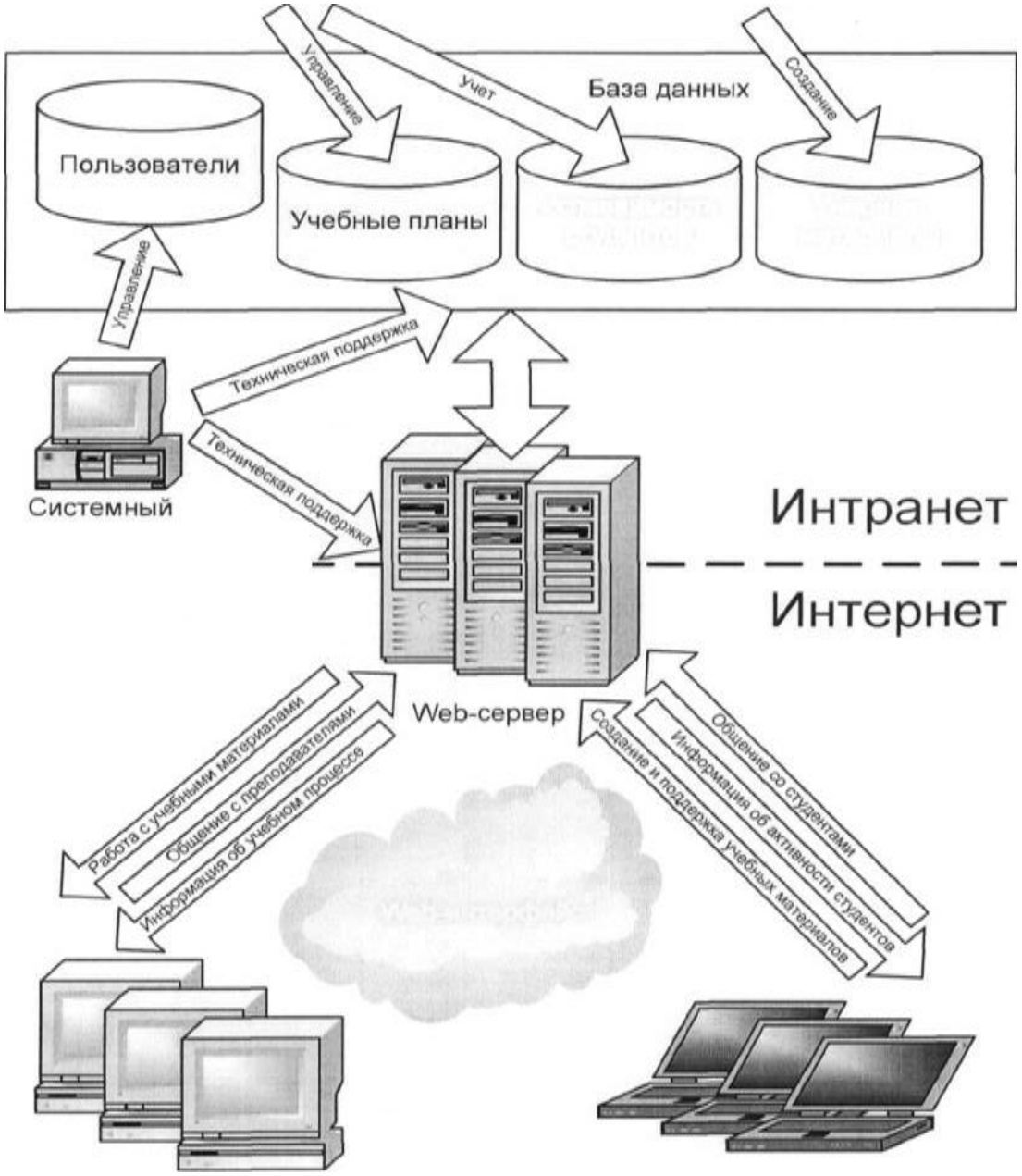



Рис.1.3.3.1. Соотношения в СДО Палестины

Сетевая безопасность должна обеспечивать различные виды доступа: использование Internet и предоставление Internet- услуг вовне, подключение по телефонным линиям (пока широко распространенным в Палестине), работу в локальной сети [14, 107,108]. Все в СДО, так или иначе, опираются на исключительно важные программные технологии, в которых мы и разработаем программы и методики.

### 1.3.4. Исследования информационных ресурсов СДО Палестины

Основой СДО является высококачественная и высокотехнологичная информационно-образовательная среда[14]. В целях решения этой проблемы и для организации управления информационными ресурсами СДО в условиях электронного документооборота необходима разработка и создание организационно-правовой структуры, предусматривающей развитие системы прогнозирования и последующего мониторинга информационных потоков, которая включала бы в себя (табл.1.3.4.1):

Таблица 1.3.4.1. Мониторинг информационных потоков

| Процесс | Кто обеспечивает |
|---|---|
| перепись, регистрацию и учет основных информационных массивов | Тьюторы, администрация, администраторы сети |
| классификацию информационных массивов по максимально возможному числу параметров | Тьюторы, администраторы сети |
| анализ процессов движения (потребления) информационных ресурсовв СДО и разработку рекомендаций по повышению эффективности их использования | Тьюторы, администраторы сети |
| обеспечение условий государственного регулирования | администрация, администраторы сети |

| | |
|---|---|
| информационных взаимодействий на основе лицензионной системы | |

При формировании информационной среды СДО необходимо также установить порядок включения в нее информационных ресурсов с ограниченным доступом и предусмотреть создание в рамках СДО соответствующих организационно-правовых механизмов и разработку нормативно-методических документов, определяющих основную деятельность в образовательном учреждении (таьл.1.3.4.2):

Таблица 1.3.4.2. Организационно-правовые механизмы СДО

| Основной процесс | Кто обеспечивает |
|---|---|
| порядок отнесения сведений к категории ограниченного доступа | администрация |
| порядок организации работы, состав и правомочия тьюторов | Тьюторы, администрация, администраторы сети |
| критерии формирования перечней сведений конфиденциального характера, порядок и сроки их пересмотра | администрация, администраторы сети |
| порядок обмена этими сведениями при различных нормах отображения информации на материальных носителях | администраторы сети |
| порядок оформления допуска и доступа к указанным сведениям | Тьюторы, администраторы сети |
| механизмы реализации различных видов юридической ответственности за неправомочные действия | администрация |

При разработке и реализации СДО как составляющей части единой образовательной информационной среды должен быть решен вопрос о создании специальной подсистемы защиты информации [14,70] как неотъемлемой составляющей части всей системы дистанционного обучения. Перед подсистемой защиты информации должны быть поставлены следующие конкретные задачи (табл.1.3.4.3):

Таблица 1.3.4.3. Основные задачи в СДО

| Задачи | Кто обеспечивает |
|---|---|
| защита ресурсов системы дистанционного обучения от несанкционированной установки, копирования, модификации и использования, обеспечение их целостности и подлинности | администрация, администраторы сети |
| авторизация персонала, управляющего функционированием системы | администраторы сети |
| авторизация преподавателей и обучающихся в процессе их взаимодействия | Тьюторы, студенты, администраторы сети |
| разграничение прав доступа авторизованных пользователей системы к ее ресурсам, основанное на разделении субъектов и объектов по полномочиям, группам, категориям и тематикам | администрация, администраторы сети |

Наконец, обеспечение информационной безопасности информационной среды СДО теснейшим образом связано с информационной безопасностью сетевых систем [14,74].

Основными результатами работы должны стать (табл.1.3.4.4).

Таблица 1.3.4.4. Задачи и результаты защиты в СДО Палестины

| Задачи, результаты | Кто участвует | Ответственный |
|---|---|---|
| Повышение качества обучения в СДО | Тьюторы, студенты, администрация, партнеры, администраторы сети | Тьюторы, администрация, администраторы сети |
| Доступ учащихся и преподавателей из других учебных заведений к информационным ресурсам СДО | Тьюторы, студенты, партнеры, администраторы сети | Тьюторы, администраторы сети |
| Развитие персонализации процесса обучения на основе организации индивидуальных образовательных траекторий | Тьюторы, студенты | Тьюторы, администрация, администраторы сети |
| Предоставление условий для полноценного образования, необходимого специального обучения различным группам населения | Тьюторы, студенты, партнеры, | Тьюторы, администрация, администраторы сети |
| Создание единой системы обеспечивающей | Тьюторы, студенты, администраторы | Тьюторы, администрация, |

| | | |
|---|---|---|
| информационную и научно-методическую поддержку образовательного процесса, оказание консультационных услуг | сети | партнеры, администраторы сети |
| Повышение отвечающего современным требованиям уровня подготовки в области информационных технологий | Тьюторы, администрация, администраторы сети | Тьюторы, администрация, администраторы сети |

### 1.4.Информационная безопасность и основные проблемы при создании СДО в Палестине

Либерализация и открытие рынка телекоммуникаций (и мобильная и стационарная линия) делают Палестину уникальной окружающей средой для инвестиций в телекоммуникации и уже привлекли существенные иностранные инвестиции.

Информационная безопасность и финансовые проблемы являются особенностью двадцать первого века, и, практически не существует таких государств, которые не сталкивались бы с ними. Инвесторам предоставляются различные выгоды, которые создают привлекательную деловую инвестиционную среду и импортированные основные фонды освобождены от таможенных пошлин и налогов на 100 %, и импортированные запасные части для основных фондов освобождены от выплат и налогов до 15 % общей стоимости вне оборотных активов[14,107,108].

Структуру СДО ППУ с точки зрения организации процесса обучения покажем на рис. 1.3.5.1


Рис.1.3.5.1.Структура СДО ППУ

### 1.4.1. Информация в беспроводных сетях СДО Палестины

При проектировании СДО администраторы забывают, что хакеры могут подключиться к сети откуда угодно[14, 107,108]. Сам принцип беспроводной передачи данных заключает в себе возможность несанкционированных подключений к точкам доступа. Защиту информации при подключении к СДО таких устройств неквалифицированные сотрудники обеспечивают иногда самостоятельно. Решением подобных проблем нужно заниматься комплексно[14,107,108], что мы и предлагаем и разрабатываем в нашей работе. Существует распространенное заблуждение, что применение уникального Service Set ID (SSID) позволяет избежать несанкционированных подключений. Увы, SSID пригоден лишь для логического разбиения сетевых устройств на группы.

Мы далее покажем более прогрессивные пути исправления этих проблем.

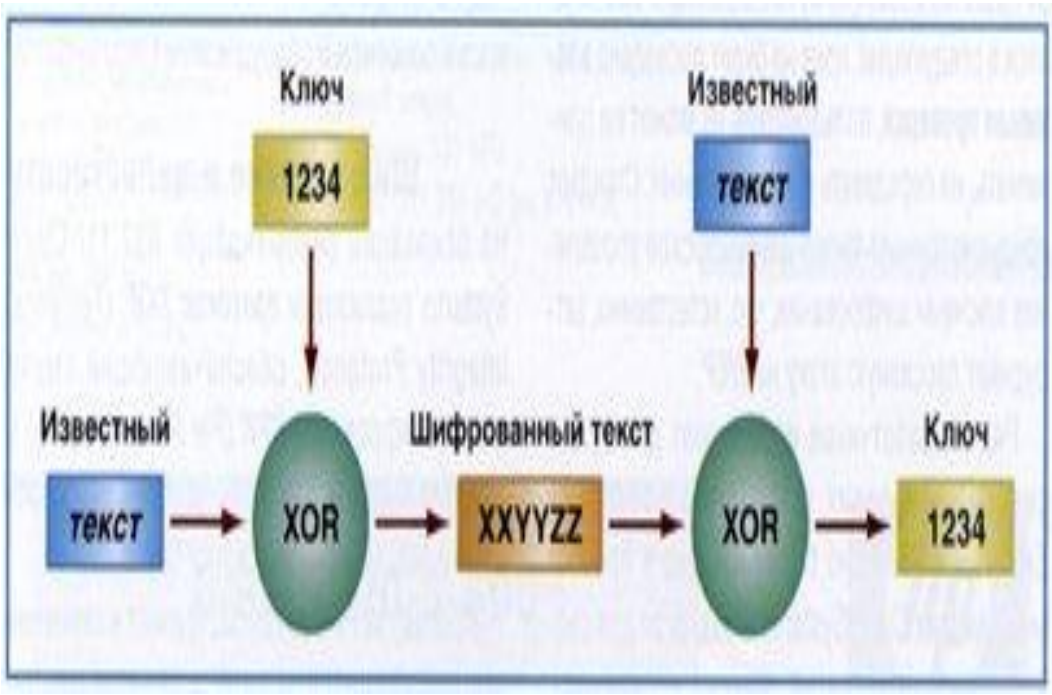



Рис.1.4.1.1. Анализ зашифрованных данных в СДО Палестины

Все вышесказанное позволяет говорить о ненадежности старых методов обеспечения безопасности в беспроводных сетях СДО Палестины, поэтому в

тех случаях, когда имеющееся оборудование не позволяет реализовать современные решения по защите информации, необходимо либо использовать строжайшую административную политику, либо применять технологию IPSec-ESP, которая даст возможность надежно защитить данные, однако заметно снизит производительность ЛС [14].

Мы далее покажем более прогрессивные подходы.

### 1.4.2. Аутентификация

В настоящее время в различном сетевом оборудовании, в том числе в беспроводных устройствах, широко применяется более современный по сравнению со стандартами 2007-2008 годов способ аутентификации, который отличается от прежних способов аутентификации в следующем: пока не будет проведена взаимная проверка пользователь не может ни принимать, ми передавать никаких данных. Стандарт предусматривает также динамическое управление ключами шифровании, что, естественно, затрудняет пассивную атаку на WEP. Ряд разработчиков используют для аутентификации в своих устройствах протоколы EAP-TLS и PEAP, но более широко к проблеме подходит Cisco Systems, предлагая для своих беспроводных сетей, помимо упомянутых, следующие протоколы (табл.1.4.2.1):

Таблица 1.4.2.1. Стандарты и протоколы по обеспеченности и по ответственности

| Стандарты, протоколы | Обеспечение | Ответственный |
|---|---|---|
| EAP-TLS - стандарт IETF | обеспечивает аутентичность путем двустороннего обмена цифровыми сертификатами | Разработчик, администратор сети, |
| PEAP - пока предварительный стандарт (draft) IETF | предусматривает обмен цифровыми сертификатами и | Разработчик, заказчик, администратор сети |

| | | |
|---|---|---|
| | дополнительную проверку имени и пароля по специально созданному шифрованному туннелю | |
| LEAP - фирменный протокол Cisco Systems | Использует разделяемый ключ, поэтому требует продуманной политики генерации паролей | заказчик, администратор сети, тьюторы |
| EAP-FAST - разработан Cisco на основании предварительного стандарта (draft) IETF | для защиты от атак по словарю и имеет высокую надежность. Принцип работы схож с LEAP, но аутентификация производится по защищенному туннелю | заказчик, администратор сети, |

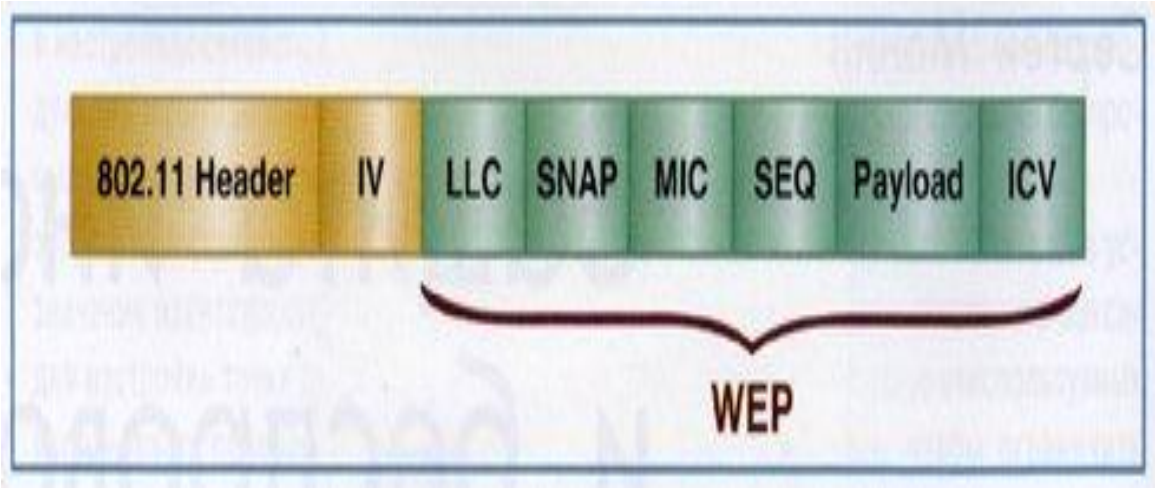



Рис.1.4.2.1. Схема пакета в СДО Палестины

Из нашего опыта и из опыта Аль- Агбари [14] рекомендуется распределять пользователей с разной степенью защищенности по разным виртуальным ЛС и в соответствии с этим реализовывать свою политику безопасности[105-108].

Таблица 1.4.2.2. Аутентификации и ее особенности

| **Показатель** | **Способ** | | | |
|---|---|---|---|---|
| | **LEAP** | **EAP-FAST** | **PEAP** | **EAP-TLS** |
| Поддержка современных ОС | Да | Да | Не все | Не все |
| Сложность ПО и ресурсоёмкость аутентификации | Низкая | Низкая | Средняя | Высокая |
| Сложность управления | Низкая | Низкая | Средняя | Средняя |
| Single Sign on (единый логин в Windows) | Да | Да | Нет | Да |
| Динамические ключи | Да | Да | Да | Да |
| Одноразовые пароли | Нет | Да | Да | Нет |
| Поддержка баз пользователей не в формате MS Windows | Нет | Да | Да | Да |
| Fast Secure Роуминг | Да | Да | Нет | Нет |
| Возможность локальной аутентификации | Да | Да | Нет | Нет |

## 1.5. Выводы по главе 1

1. Показана актуальность систем дистанционного обучения для Палестины.
2. Рассмотрены основные проблемы в СДО, известные пути их решения и основные нерешенные проблемы.
3. Обоснована необходимость защиты телекоммуникаций СДО от несанкционированного доступа к информации с учетом особенностей Палестины поскольку известные методики не обеспечивают необходимое качество.
4. При планировании защищенной беспроводной сети , любое шифрование или другие манипуляции с данными неизбежно приводят к дополнительным задержкам, увеличивают объем служебного трафика и нагрузку на процессоры сетевых устройств. Безопасность - безусловно, важный фактор в современных сетях, но он теряет всякий смысл, если трафик пользователя не получает должной полосы пропускания. Сети создаются, в конечном счете не для администраторов, а для пользователей.

# ГЛАВА 2. СИНТЕЗ ЗАЩИЩЕННЫХ СТРУКТУР СДО И УЛУЧШЕНИЕ ИХ ХАРАКТЕРИСТИК

## 2.1. Проникновения в информационные сети СДО

Для СДО Палестины актуально обнаружение электронных устройств перехвата информации (закладных устройств), так же как и любых других объектов, по их демаскирующим признакам.

Каждый перехват информации имеет свои специфические признаки, позволяющие обнаружить закладку. Подробнее см. приложения.

Необходимо использовать информативные признаки проводной и беспроводной систем демаскирующие признаки не камуфлированных акустических закладок [74,75,89,90] , а для акустических и телефонных закладок с передачей информации по телефонной линии на ВЧ демаскирующие признаки [74,90].

Методики поиска закладных устройств во многом определяются использованием той или иной аппаратуры контроля. К основным методикам поиска посторонних закладных устройств относят [89,90, 107,108]. Мы их свели в табл.2.1.1:

Таблица 2.1.1. Поиск закладных устройств НСД

| Поиск устройств НСД | Обеспечение |
|---|---|
| специальное (утвержденное) обследование выделенных помещений | Администратор сети, администрация, инженер по защите информации |
| поиск закладок с использованием индикаторов поля, частотомеров и интерсепторов | Администратор сети, инженер по защите информации |
| поиск закладок с использованием программно-аппаратных комплексов контроля | Администратор сети, инженер по защите информации |
| поиск закладок с использованием специальных сканерных приемников и анализаторов спектра | инженер по защите информации |
| поиск и устранение портативных звукозаписывающих устройств с использованием детекторов диктофонов [74] | инженер по защите информации |
| поиск видеозаписывающих устройств по наличию различных побочных излучений, связанных с принципами действия видеокамер | инженер по защите информации |
| поиск закладок с использованием нелинейных локаторов | администрация, инженер по защите информации |
| поиск закладок с использованием рентгеновских комплексов | администрация, инженер по защите информации |
| проверка с использованием ВЧ - пробника линий электропитания, радиотрансляции и телефонной связи | инженер по защите информации |
| измерение контроль различных параметров линий электропитания, телефонных линий | инженер по защите информации, представитель |

| | |
|---|---|
| связи | электросети, представитель телефонной компании |
| проведение тестовых проверок всех телефонных аппаратов, установленных в проверяемом помещении, с контролем прохождения всех вызывных сигналов АТС, аналогично и для мобильных | инженер по защите информации, представитель телефонной компании |

Подробнее см. приложения.

Идентификация обнаруженного объекта является наиболее сложной частью работы и требует от оператора навыков в работе и внимания.

Учитывая определенные трудности в поиске вредоносных устройств НСД и большие потери времени и средств для этого, целесообразно защищать сети СДО на этапе проектирования и специально готовить инженеров по защите информации, которые должны быть или в штате СДО или в штате специализированных компаний.

## 2.2. Проектирование структуры СДО для информационной защиты сети

Для целей зашиты сети СДО от несанкционированного доступа [99] нами создана подсистема, позволяющая решать задачи:

-установление роутеров, как проводных так и беспроводных: Устройство локализует маршрутизаторы в узлах графа пересечения канала для общей топологической структуры системного уровня. Для этого нами разработан алгоритм для ядра в стадии преобразования всей совокупности роутеров.

-Создание последовательности и проектирование структуры: Объединение маршрутов для всех путей завершает формирование структуры сети. Представлен алгоритм приближения, который маршрутизирует пути и синтезирует структуру таким образом, чтобы расход энергии был

минимален, и чтобы необходимое число роутеров в сети СДО было бы максимум в 2 раза больше, чем в оптимальном решении[99].

-Слияние роутера: предпоследний шаг в стадии проектирования соединяет близко находящиеся роутеры в один, при условии, что ограничения длины канала передачи данных не нарушены.

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

На рис.2.2.1 показано схематично проектирование специализированного приложения для ускорения синтеза сети СДО и увеличения ее эффективности.

Практическая проверка, проведенная нами при внедрении в сеть СДО Палестинского университета(см. приложение).

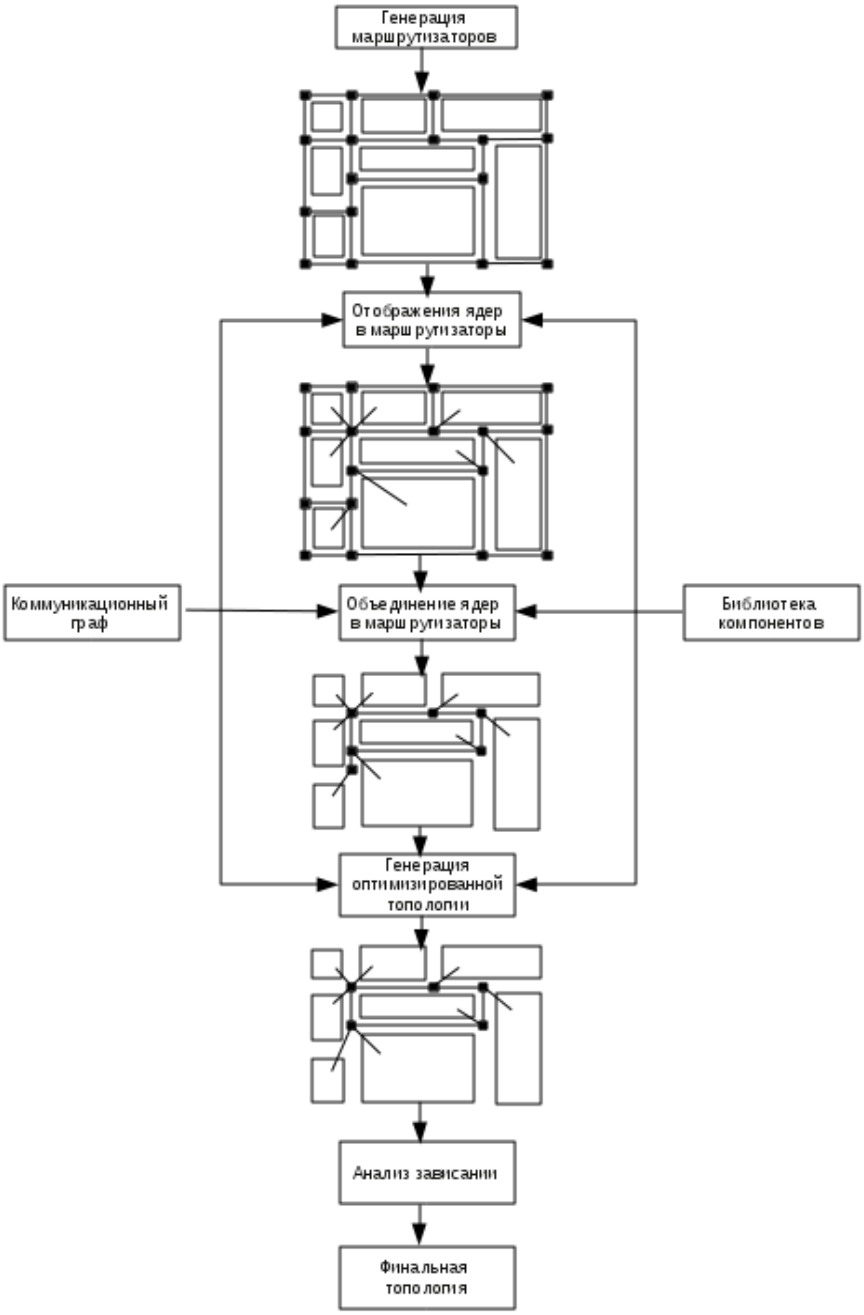



Рис.2.2.1. Схематичное проектирование специализированного приложения

В качестве среды программирования для реализации подсистемы проектирования нами была выбрана система инженерных и научных вычислений MATLAB, хорошо себя показавшую в Палестине. А так же использовался язык программирования C++.

Главными при выборе MATLAB было:

- 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, хорошо освоенная в Палестине, 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. Поэтому и выбрана нами в этом проектировании.

Комплекс программ подсистемы САПР проектирования состоит из основной вызываемой программы и ряда дополнительных подпрограмм, которые реализованы в виде М-файлов. Структура любой функции, оформленной как М-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.

```
// 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;
}
```

КОНСОЛЬНОЕ ПРИЛОЖЕНИЕ. Обзор проекта

Это приложение создано автоматически с помощью мастера приложений.

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

aaaa.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.

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

46) I[i]=-0.201774  l[45]=0.046

47) I[i]=-0.205007  l[46]=0.047

48) I[i]=-0.208215  l[47]=0.048

49) I[i]=-0.211399  l[48]=0.049

50) I[i]=-0.214559  l[49]=0.05

51) I[i]=-0.217695  l[50]=0.051

52) I[i]=-0.220809  l[51]=0.052

53) I[i]=-0.223899  l[52]=0.053

Разработанный программный комплекс представляет собой подсистему САПР, реализованную по агрегатному принципу на основе открытой архитектуры СДО, что позволяет легко осуществлять ее наращивание. Что важно при модификациях системы. Структура комплекса представлена на рис. 2.2.2. Выбор данной концепции при создании подсистемы СДО был сделан, исходя из критерия универсальности и легкости модификации и дополнения комплекса каждым конечным пользователем при решении своих конкретных 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 СДО в настоящее время, имеют закрытую архитектуру, что делает невозможным доступ пользователя к внутренним массивам данных этих систем.

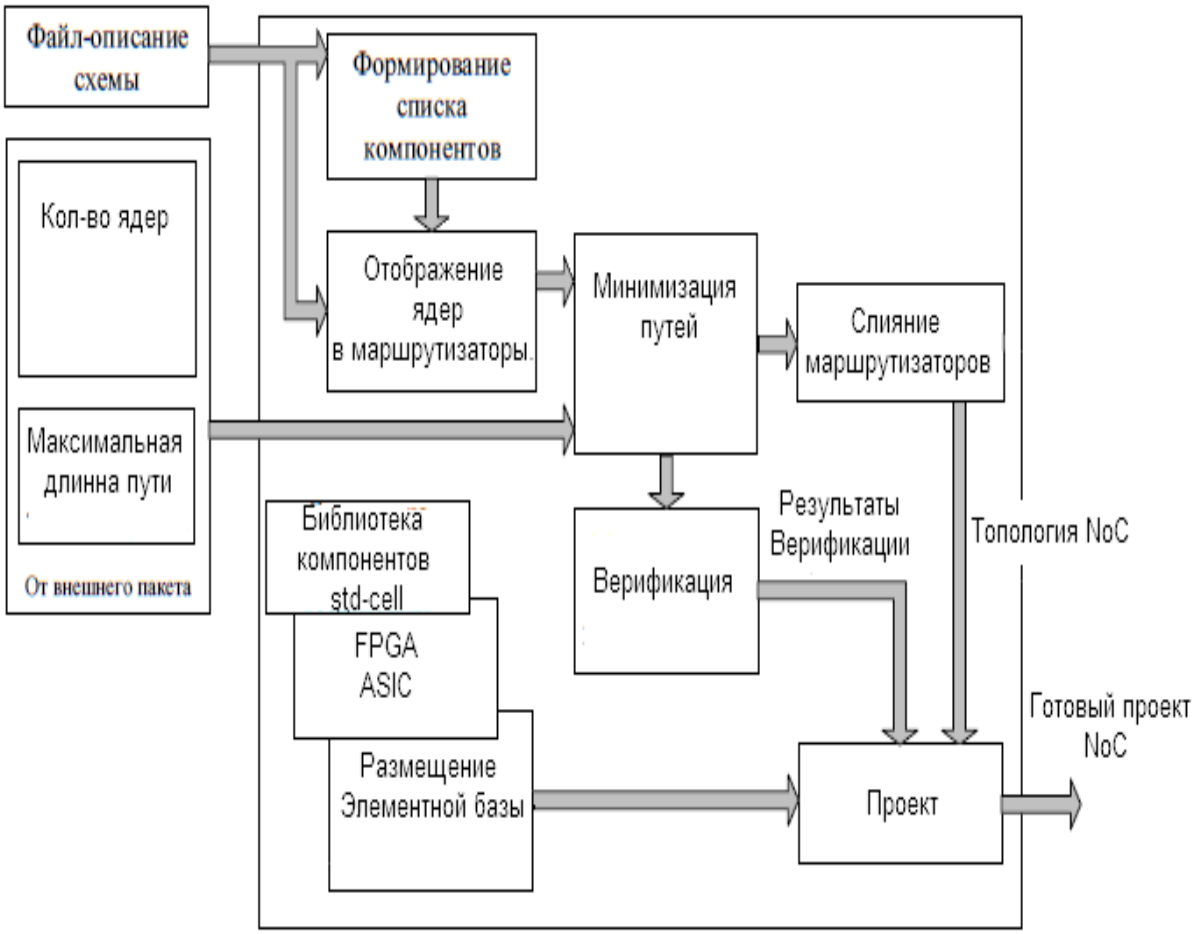



Рис.2.2.2 Структура представляет собой подсистему САПР СДО

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

- работа с проектом (на всех стадиях);
- генерация топологии защищаемой сети, в наиболее удобном виде;
- поиск неисправности или несанкционированного проникновения в сеть[1,2];
-экспорт в САПР для конкретной СДО.

**2.3. Оптимизация структур при обеспечении информационной защиты в сетях СДО**

Поскольку в образовательной сети может оказаться много роутеров (как проводных так и беспроводных), считаем необходимым уменьшение их до целесообразного(оптимального) количества и поэтому разработаем соответствующий алгоритм[98]

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

Строится матрица 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.

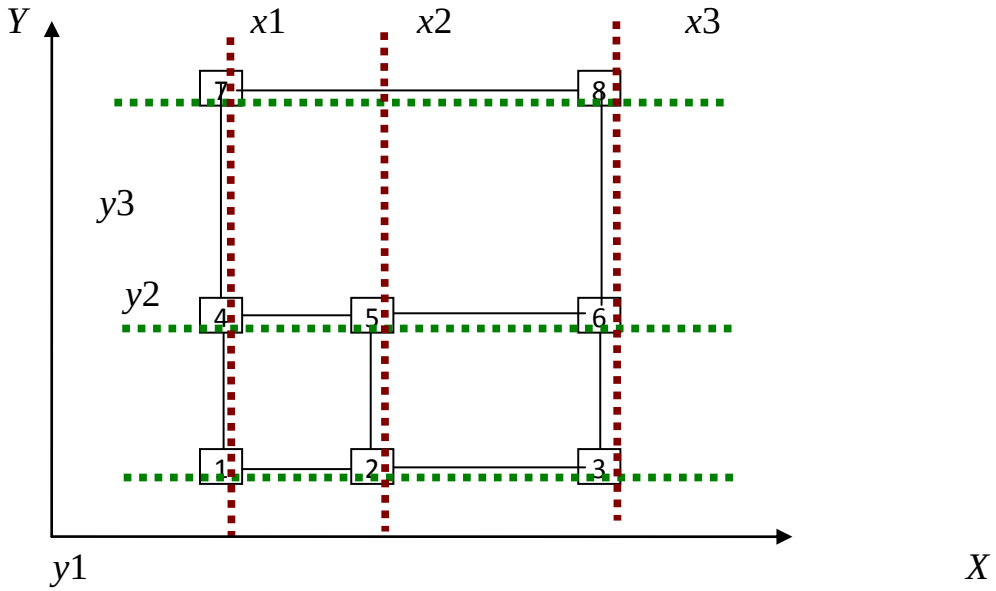
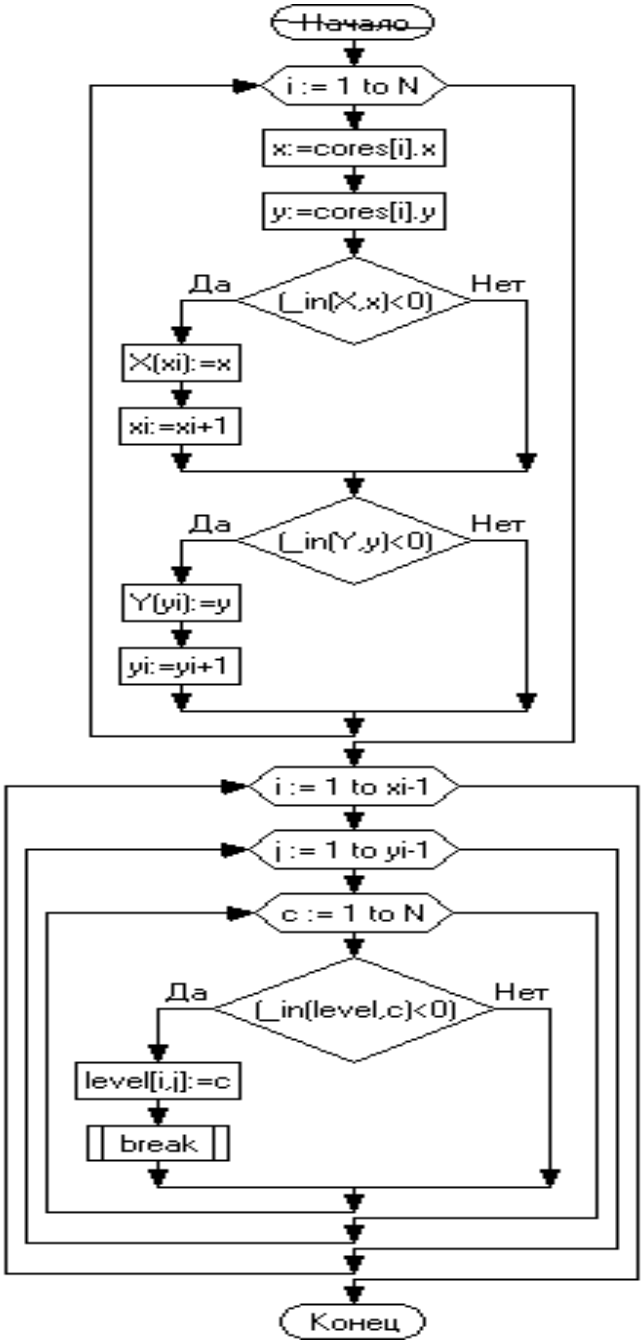



Рис 2.3.1. Уровни ядер в сети

Чтобы построить матрицу *L* достаточно найти все уровни *x* или *y*. Их можно найти по следующему алгоритму:1.Возьмем *i*-е ядро. 2.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. В итоге получим матрицу *L*. И количество уровней *x* – *X*

(количество строк в матрице), и количество уровней *y* – *Y* (количество столбцов). Блок схема алгоритма:




После построения матрицы уровней *L*, находим начало будущих роутеров. Роутеры лучше всего строить с левого нижнего угла (проверено нами на практике, при внедрении). 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”. Укажем, что наличие соседей справа и сверху - необходимое, но не достаточное. 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. 2.3.2). 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 $L(i + 1, j + k)$ 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. Это мы хорошо увидели при проектирования сети СДО Палестинского университета. Поэтому и рекомендуем заинтересованным лицам.

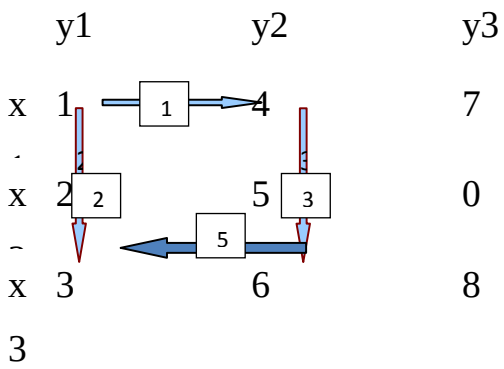



Рис.2.3.2. Номера на стрелках указывают порядок действий.

Возьмем ядро 1. Оно находится на уровне *x*1 и *y*1. Ищем его соседей 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. То есть для всей структуры.

После построения структуры получаем массив роутеров *R*. Каждый *R(i)* элемент которого, роутер и ядра, которые входят в него.

По разработанному нами алгоритму строятся все возможные роутеры. Уменьшение ресурсов роутеров приводит к сокращению статического расхода энергии и облегчению проектирования структуры сети СДО и верификации. Мы можем уменьшить их количество путем объединения соседних роутеров в сети. При этом объединении нужно проводить таким образом, чтобы не пропадали ядра (см. пример на рис. 2.3.3). И длина пути не оказалась больше максимально разрешенной длины пути *D* в данной структуре. И чтобы сеть не потеряла своей функциональности и обеспечивала все требуемые задачи, установленные заказчиком.

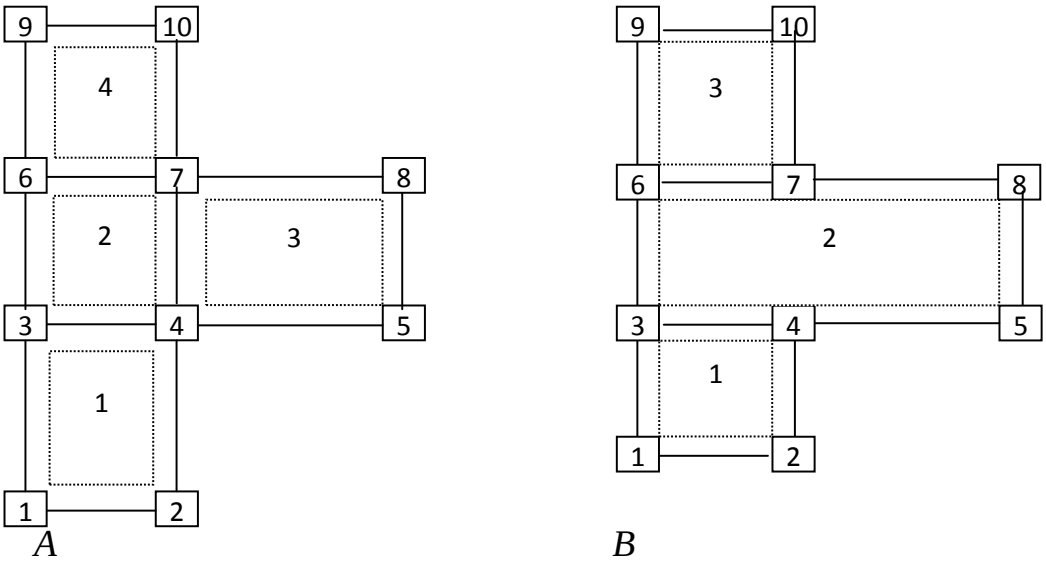
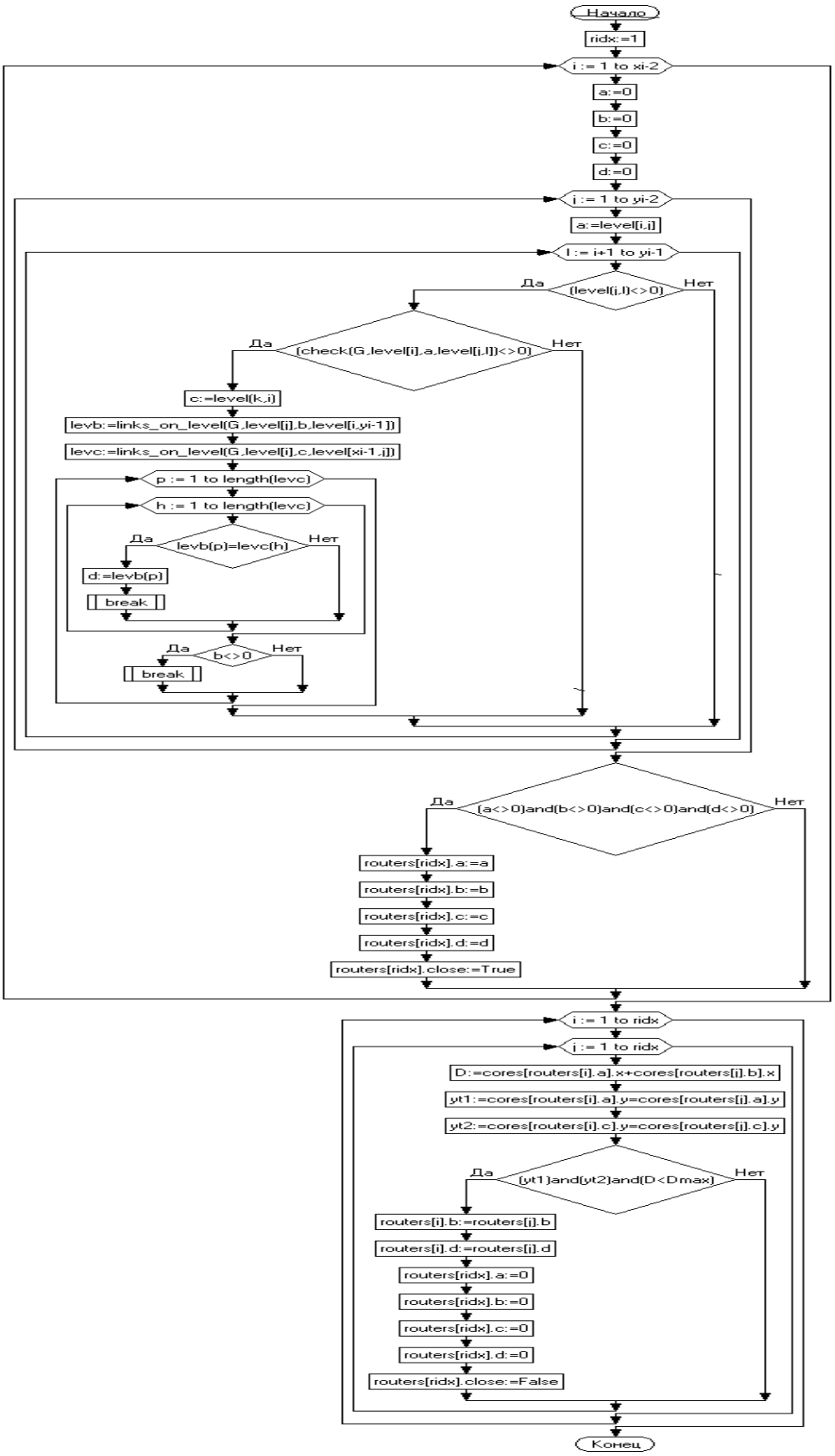



Рис 2.3.3. Объединение роутеров. *A* — до объединения, *B* — после.




На рис.2.3.3 изображены 10 ядер, связи между ними и 4 роутера.

Блок-схема алгоритма построения роутеров и уменьшения их количества.

Как мы установили при внедрении в Палестинском университете, наша разработка позволяет и сократить время проектирования структуры и ощутимо уменьшить энергетические затраты в сети СДО.

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 объединяются следующим образом.

Возьмем R(i) роутер, и соседние, если их ядра лежат на одинаковых x или y уровнях, тогда эти роутеры можно объединить в один.

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

Следовательно, после объединения получаем существенно уменьшенное количество роутеров.

Нами было предложено [98], что у каждого ядра есть только один порт ввода/вывода (*I/O*), который должен быть присоединен к единственному порту роутера.

// 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 #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>

По существу, каждый порт ядра должен быть смоделирован отдельным узлом в потоковом графе, чтобы решить этот вопрос[98,99]. Это нами проверено при внедрении в сети СДО Палестинского университета.

## 2.4. Обеспечение информационной безопасности GSM при использовании в СДО Палестины

В Палестине широко используются телефонные сети различных стандартов для целей СДО. Рассмотрим обеспечение их информационной безопасности применительно к Палестинскому университету.

Идентификатор PIN-код, известный только абоненту, который должен служить защитой от несанкционированного использования SIM-карты, например, при ее утере. После трех неудачных попыток набора PIN-кода SIM-карта блокируется, и блокировка может быть снята либо набором дополнительного кода — персонального кода разблокировки (Personal Un-blocking Key — PUK), либо по команде с центра коммутации.

Процедура аутентификации стандарта GSM схематически показана на рис.2.4.1.

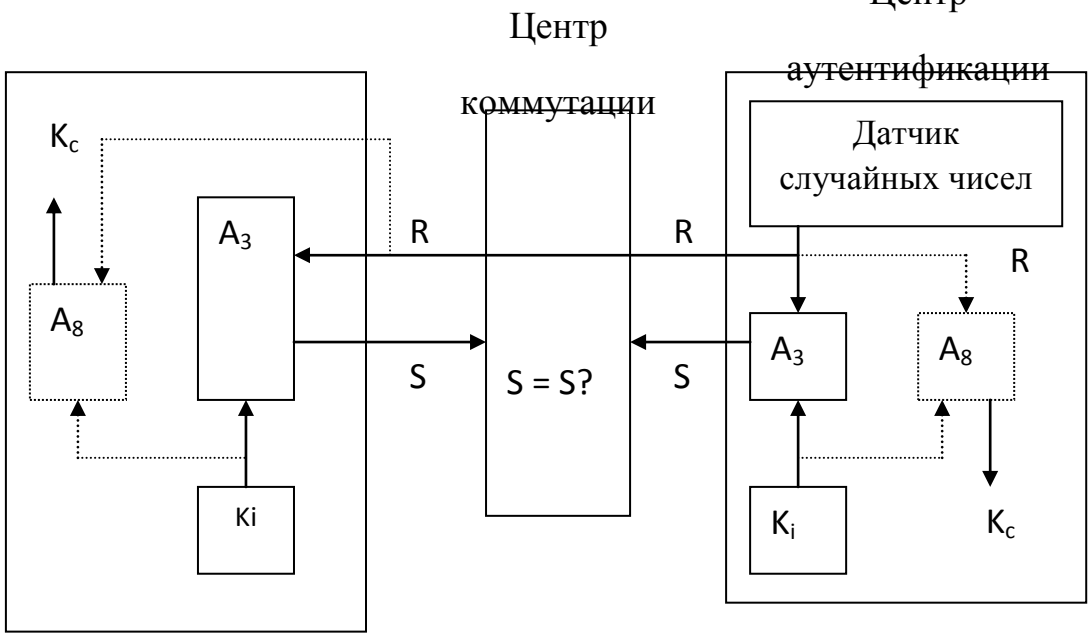



Рис. 2.4.1. Аутентификация в GSM; А3 — алгоритм аутентификации; А8 — алгоритм вычисления ключа шифрования; Ki — ключ аутентификации; Кс — ключ шифрования; S — зашифрованный отклик(Signed Response-SRES).

Вычисление производится каждый раз при аутентификации.

Идентификатор должен соответствовать таким требованиям, чтобы его изменение или подделка были трудными и/или экономически дорогими.

## 2.5. Выводы по главе 2

1. Рассмотрены известные методы и устройства для поиска несанкционированных проникновений в телекоммуникации, в том числе и в СДО с учетом особенностей Палестины.
2. Разработаны алгоритмы синтеза сетей с роутерами (маршрутизаторами) и их минимизации.
3. Приведены основные проблемы защиты информации в GSM для СДО.
4. Проанализированы основные особенности защиты информации применительно в Палестине.
5. Разработаны методики и алгоритмы минимизация роутеров (маршрутизаторов) на этапе проектирования что позволяет уменьшить аппаратурные затраты более чем в 2 раза (см. Приложения 2).

# 3. МЕТОДИКА ОЦЕНКИ ЦЕЛЕСООБРАЗНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ СДО ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Как отмечалось, для каждого типа угроз может быть одна или несколько мер противодействия (см. п.1). В связи с неоднозначностью выбора мер противодействия необходим поиск некоторых критериев, в качестве которых могут быть использованы надежность обеспечения сохранности информации и стоимость реализации защиты. Принимаемая мера противодействия с экономической точки зрения будет приемлема, если эффективность защиты с ее помощью, выраженная через снижение вероятного экономического ущерба, превышает затраты на ее реализацию[74]. В этой ситуации можно определить максимально допустимые уровни риска в обеспечении сохранности информации и выбрать на этой основе одну или несколько экономически обоснованных мер противодействия, позволяющих снизить общий риск до такой степени, чтобы его величина была ниже максимально допустимого уровня, заданного заказчиком. Из этого следует, что потенциальный нарушитель, стремящийся с пользой для себя применить предоставленные ему возможности, не будет тратить на выполнение угрозы больше, чем он ожидает выиграть. Следовательно, необходимо поддерживать цену нарушения сохранности информации на уровне, превышающем ожидаемый выигрыш потенциального нарушителя. Рассмотрим эти подходы. Утверждается, что большинство разработчиков средств вычислительной техники рассматривает любой механизм аппаратной защиты как некоторые дополнительные затраты с желанием за их счет снизить общие расходы. При решении на уровне руководителя проекта вопроса о разработке аппаратных средств защиты необходимо учитывать соотношение затрат на реализацию процедуры и достигаемого уровня обеспечения сохранности информации. Поэтому разработчику нужна

некоторая формула, связывающая уровень защиты и затраты на ее реализацию, которая позволяла бы определить затраты на разработку потребных аппаратных средств, необходимых для создания заранее определенного уровня защиты. В общем виде такую зависимость задают исходя из следующих соображений. Если определять накладные расходы, связанные с защитой, как отношение количества использования некоторого ресурса механизмом управления доступом к общему количеству использования этого ресурса, то экономические методы управления доступом дадут накладные расходы, приближающиеся к нулю.

### 3.1. Обоснование мероприятий по защите от несанкционированного доступа в сетях СДО Палестины

При оценке необходимости защиты СДО от несанкционированного доступа к информации обосновано считается, что полные затраты (потери) определятся выражением, предложенным Галкиным А.П., которое нужно минимизировать[74]

$$R_{затр} = r_{пот} P_{пи} P_{нпи} + r_{мер} P_{опи} P_{оопи} \rightarrow \min,$$

Параметры с учетом их использования и тем, кто их определяет или задает разместим в табл. 3.1.1.

Таблица 3.1.1. Параметры: определение и назначение

| Обозначение | Параметр | Назначение, определение |
|---|---|---|
| Rапп. | затраты на аппаратуру | Проект, администрация, заказчик |
| Rэкс. | эксплуатационные затраты | администрация |
| R реж. | затраты на организацию режима ВУЗе | Администрация |

| | | |
|---|---|---|
| Рпи | вероятность потерь информации | Заказчик |
| $Р_{нпи}$ | условная вероятность не обнаружения потерь информации | Заказчик |
| $Р_{опи}$ | вероятность отсутствия потерь информации | Заказчик |
| $Р_{оопи}$ | условная вероятность ошибки в обнаружении потерь информации | При этом надо учитывать, что $Р_{нпи} \to 1$ при отсутствии диагностики, а $Р_{оп} \to 0$ при полной диагностике |
| $Р_{нпи}=1-\sum_{i=1}^{N} P_i$ | Вероятность не обнаружения потерь информации (проникновения) | администрация, заказчик |
| $P_1=0,1$ | при установке аппаратуры по защите от подслушивания в помещении | Проект, заказчик |
| $P_2=0,1\text{-}0,2$ | при установке аппаратуры по защите от подслушивания по телефону | Проект, заказчик |
| $P_3=0,1\text{-}0,2$ | при проведении мероприятий по защите компьютерных сетей | Заказчик |
| $P_4=0,1$ | при введении режима в учебном заведении | Проект, администрация, заказчик |
| $P_5=0,1$ | при защите от несанкционированной записи | администрация, заказчик |
| $Р_{оопи}=1-\sum_{i=1}^{N} P_i$ | вероятность ошибки в обнаружении потерь информации (проникновении) (приближенно) | Проект, заказчик |

Используем опыт нескольких учебных заведений и предприятий (и наших внедрений на них), можно считать[74,75, 107,108]

Учитывая необходимость минимизации выражения полных потерь, целесообразность использования защиты будет при соблюдении условия

$R_{пот}\ P_{пи}\ P_{нпи} > r_{мер}.P_{опи}\ P_{оопи}$.

Приближено, это можно определить по формуле

$R_{пот.}P_{пи}\ P_{нпи} = kr_{мер.}(1-P_{пи})P_{оопи}$ .

При этом $k=(2-5)$ и он выбирается больше при большем вложении в это учебное заведение (страховочный подход)[74].

Такой подход в оценке целесообразности защиты информации в учебном заведении правомерен на предварительном этапе решения, поскольку не требует большого количества данных, а только указания и пожелания заказчика.

### 3.2. Оценка эффективности информационного канала СДО

Приведем известные критерии, предложенные Галкиным А.П.[74,75]:

$$\max Эм = \frac{П_{\Sigma}}{З_{с} + З_{экс}} \qquad (3.2.1)$$

$$\max \left\{П_{\Sigma}\right\} \Big/ (З_{с} + З_{экс}) \le З_{с} \qquad (3.2.2)$$

$$\frac{\min\{Зс + Зэкс\}}{П_{\Sigma}} \le П\,зад \qquad (3.2.3)$$

$$\frac{\max\{П_{\Sigma}\}}{\min\{Зс + Зэкс\}} \qquad (3.2.4)$$

Наиболее объективная форма – (3.2.4), → количественная форма – (3.2.1). В данном подходе под ЭМ понимается комплексный критерий качества модели [75]. Покажем это в табл.3.2.1.

Таблица 3.2.1.Требования к показателю качества модели:

| Требования, свойства | Кто задает |
|---|---|
| определять в какой степени модель позволяет достигнуть поставленной цели в обучении и в оценке тьюторов | Заказчик, руководитель проекта |
| быть количественным, чтобы сравнение моделей было обоснованным и понятным | Заказчик, руководитель проекта |
| быть устойчивым, т.е. иметь малый разброс в измеренных значениях | администратор сети, руководитель проекта |

Чаще всего при оценке ЭМ понимают только адекватность, забывая о том, что затраты на различные варианты моделей могут существенно отличаться.

Для большей объективности целесообразно оценивать ЭМ интегральным критерием[75]:

$$\text{Эм} = \frac{\text{П}_\Sigma}{\text{Зс} + \text{Зэкс}},$$

где $\text{П}_\Sigma$ – суммарный полезный эффект;

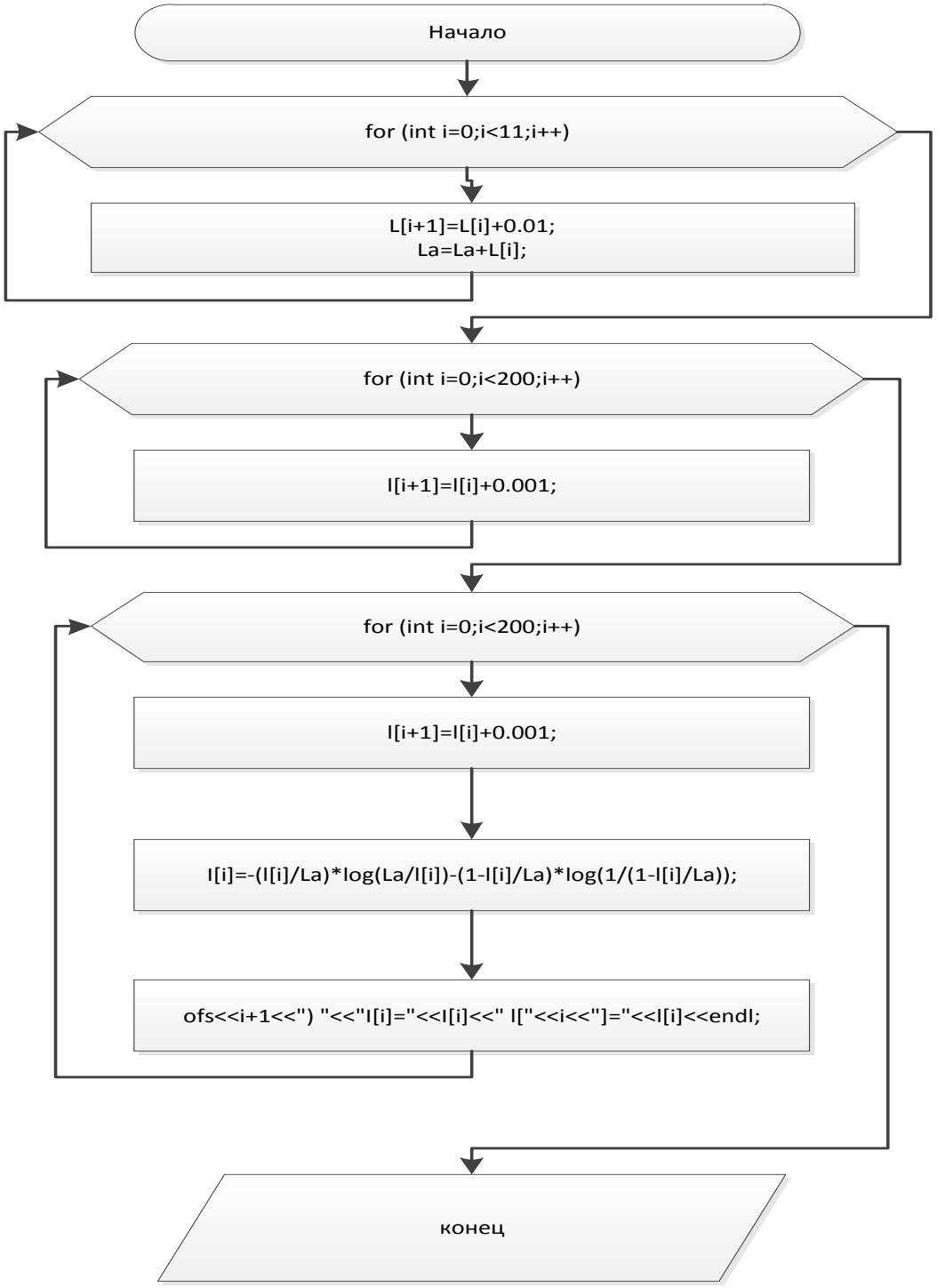
Зс и Зэкс – затраты на создание и эксплуатацию модели соответственно.

В инженерной практике могут найти применение следующие разновидности индексных критериев, как это показано в [75] и проверено нами при внедрениях (см. Приложения), удовлетворяющие указанным условиям [107,108], приведенным в табл.3.2.2:

Таблица 3.2.2. Индексные критерии и условия удовлетворения

| Критерии | Условия |
|---|---|
| $Эм = \frac{\sum_{i=1}^{S} n_i q_i L_i}{\sum_{i=1}^{S} n_i L_i}$ | $C_i = n_i L_i$; $C = \sum_{i=1}^{S} n_i L_i = \sum_{i=1}^{S} C_i$, |
| $Эм = \frac{\sum_{i=1}^{S} q_i C_i}{C}$ | $q_i$ – относительный критерий, например вида: $q_i = \frac{p_i}{p_{iб}}$ |
| $Эм = \frac{\sum_{i=1}^{S} \alpha_i q_i C_i}{\sum_{i=1}^{S} C_i}$ | $\sum_{i=1}^{S} \alpha_i = 1$ |
| $Э_{\Sigma} = \frac{\sum_{j=1}^{l} C_j Э_{мj}}{\sum_{j=1}^{l} C_j}$ | эффективности нескольких процессов проектирования конкретных СДО |
| $Ик = \frac{\sum_{i=1}^{S} n_i q_i L_i}{\sum_{i=1}^{S} n_i L_i}$ | $C_i = n_i L_i$, $C = \sum_{i=1}^{S} n_i L_i = \sum_{i=1}^{S} C_i$, $Ик = \frac{\sum_{i=1}^{S} q_i C_i}{C}$ |
| $Икобщ = \frac{C1Ик1 + C2Ик2 + ... + CmИкm}{C1 + C2 + ... + Cm}$ | $Ки = \frac{П_{\Sigma}}{З_С + З_{ПП}}$, $Э = \frac{\sum_{i=1}^{S} \alpha_i q_i C_i}{\sum_{i=1}^{S} C_i}$, $\sum_{i=1}^{S} \alpha_i = 1$ |

Расчетные данные для кабинетов кафедр: химии, физики, высшей математики, информатики и защиты информации Палестинского политехнического университета получаем с помощью алгоритма, разработанного нами.



Алгоритм для расчета показателей для выбора диагностируемых параметров и расчетная программа с частью результатов приведены ниже:

```
#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;
	#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[202];
float I[202];
float L[11];
float La=0;
l[0]=0.001;
L[0]=0.9;
std::ofstream ofs("tablica.txt");
for (int i=0;i<11;i++)
L[i+1]=L[i]+0.01;
La=La+L[i];
for (int i=0;i<200;i++)
l[i+1]=l[i]+0.001;
for (int i=0;i<200;i++)
l[i+1]=l[i]+0.001;
I[i]=-(l[i]/La)*log(La/l[i])-(1-l[i]/La)*log(1/(1-l[i]/La));
ofs<<i+1<<") "<<"I[i]="<<I[i]<<" l["<<i<<"]="<<l[i]<<endl;
system ("pause");
ofs.close();
return 0;
#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[202];
float I[202];
float L=0;
l[0]=0.001;
std::ofstream ofs("tablica.txt");
for (int i=0;i<200;i++)
l[i+1]=l[i]+0.001;
L=L+l[i];
ofs<<"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));
ofs<<i+1<<") "<<"I[i]="<<I[i]<<" l["<<i<<"]="<<l[i]<<endl;
system ("pause");
ofs.close();
return 0;
```

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  I[16]=0.017

18) I[i]=-0.0980391  I[17]=0.018

19) I[i]=-0.102332  I[18]=0.019

20) I[i]=-0.106566  I[19]=0.02

21) I[i]=-0.110743  I[20]=0.021

22) I[i]=-0.114865  I[21]=0.022

23) I[i]=-0.118936  I[22]=0.023

24) I[i]=-0.122957  I[23]=0.024

25) I[i]=-0.126931  I[24]=0.025

26) I[i]=-0.130858  I[25]=0.026

27) I[i]=-0.134742  I[26]=0.027

28) I[i]=-0.138584  I[27]=0.028

29) I[i]=-0.142384  I[28]=0.029

30) I[i]=-0.146145  I[29]=0.03

31) I[i]=-0.149867  I[30]=0.031

32) I[i]=-0.153553  I[31]=0.032

33) I[i]=-0.157202  I[32]=0.033

34) I[i]=-0.160816  I[33]=0.034

35) I[i]=-0.164397  I[34]=0.035

36) I[i]=-0.167944  I[35]=0.036

37) I[i]=-0.171459  I[36]=0.037

38) I[i]=-0.174943  I[37]=0.038

39) I[i]=-0.178397  I[38]=0.039

40) I[i]=-0.18182  I[39]=0.04

41) I[i]=-0.185215  I[40]=0.041

42) I[i]=-0.188581  I[41]=0.042

43) I[i]=-0.191919  I[42]=0.043

44) I[i]=-0.195231  I[43]=0.044

45) I[i]=-0.198515  I[44]=0.045

46) I[i]=-0.201774  I[45]=0.046

47) I[i]=-0.205007  I[46]=0.047

48) I[i]=-0.208215  I[47]=0.048

49) I[i]=-0.211399  I[48]=0.049

50) I[i]=-0.214559  I[49]=0.05

51) l[i]=-0.217695  l[50]=0.051

52) l[i]=-0.220809  l[51]=0.052

53) l[i]=-0.223899  l[52]=0.053

54) l[i]=-0.226967  l[53]=0.054

55) l[i]=-0.230014  l[54]=0.055

56) l[i]=-0.233039  l[55]=0.056

57) l[i]=-0.236042  l[56]=0.057

58) l[i]=-0.239025  l[57]=0.058

59) l[i]=-0.241988  l[58]=0.059

60) l[i]=-0.24493  l[59]=0.06

Результаты расчетов при внедрении разместим в табл. 3.2.7.

Таблица 3.2.7. Результирующие индексные показатели компьютерных классов ППУ

| Индексный показатель | Расчетное соотношение | Расчетный результат |
|---|---|---|
| Èê 1 | $\frac{0,1*5+0,7*3+0,9*2}{5+3+2}$ | 0,44 |
| Èê 2 | $\frac{0,4*4+0,5*5+0,6*3}{4+5+3}$ | 0,48 |
| Èê 3 | $\frac{0,2*2+0,1*3+0,3*2}{2+3+2}$ | 0,18 |

В общем случае любое моделирование (M) с такими затратами (S), чтобы $Э = \max\left\{\frac{Mi}{Si}\right\}$. Задачу идентификации конкретной СДО можно рассматривать как сопряженную по отношению к задаче управления системой. Нельзя управлять системой, если она не идентифицирована либо заранее, либо в процессе управления. Точно так же нельзя использовать модель пока не доказано соответствие ее системе.

Описание действующей СДО, когда ее структура неизвестна, формируется с помощью ее идентификации, т.е. подбора соотношений с той или иной полнотой и точностью отображающих поведение наблюдаемой

системы. Приведем найденные нами соотношения с помощью идентификации (табл.3.2.8).

Таблица 3.2.8. Идентификационные соотношения

| Критерий | Условия | Расчетное соотношение |
|---|---|---|
| $Эм = \frac{П_{\Sigma}}{Зс + Зэкс}$ | $q_i = \frac{P_i}{P_{bi}}$ | $Эм = \frac{\sum_{i=1}^{S} n_i q_i L_i}{\sum_{i=1}^{S} n_i L_i}$ |
| $Эм = \frac{\sum_{i=1}^{S} q_i C_i}{C}$ | $C_i = n_i L_i$<br>$C = \sum_{i=1}^{S} n_i L_i = \sum_{i=1}^{S} C_i$ | $Эм = \frac{\sum_{i=1}^{S} \alpha_i q_i C_i}{\sum_{i=1}^{S} C_i}; \sum_{i=1}^{S} \alpha_i = 1$ |
| $Эм = \frac{\sum_{i=1}^{S} q_i C_i}{C}$ | $\sum_{i=1}^{S} \alpha_i = 1$ | $Эм = \frac{\sum_{j=1}^{l} C_j Эмj}{\sum_{j=1}^{l} C_j}$ |

Для математического моделирования на ПК можно применять все подходы в описании и в решениях и поэтому наша математическая модель СДО, таким образом, - упрощенное и формализованное ее описание. Это нами убедительно проверено при внедрении (см. приложения).

### 3.3.Зависимость эффективности сети СДО от срывов и проникновений

Эффективность систем связи зависит, в частности, от количества и длительности срывов связи между различными абонентами и центрами и проникновений в нее[74,75].

В сложных системах связи (сетевых) большое значение имеет установление зависимости эффективности сети от срывов.

Используя известную методику из [74,75] , мы разработали инженерную методику с простыми расчетными соотношениями, которую мы убедительно проверили при внедрении (см. приложения).

Рассматриваемая сеть состоит из N абонентов (студентов и тьюторов), между i – м и j – м из которых возможна связь через определенное число каналов $K_l$ (l – число абонентов, образующий данный канал: 0,1,2,3,…, l,…, n).

Оценивать защищенность такой СДО можно, допуская ординарность любого потока событий в ней и отсутствие последействия, что чаще всего соблюдается на практике в СДО. Это позволяет считать, что средняя частота срывов связи $\lambda$ и средняя длительность времени срыва $\Delta t_{cp}$ для всех элементов – Марковский процесс[75].

Таблица 3.3.1. Результаты расчетов параметров сети для N абонентов (студентов и тьюторов)

| Критерий | Условия | Результат |
|---|---|---|
| $\sum_{l=0}^{n} K_l = n_{ji}$ | полное число каналов связи между i – м и j – м абонентами; где n – максимальное число абонентов в канале | $K_0 + \sum_{l=1}^{n} K_l \, l = N\text{-}1$ |
| $\sum_{k=1}^{l} P_k(t) = 1$<br>$P_k(t) = \frac{\lambda^k}{k!\,\mu^k} P_o(t)$ | $P_0(t)$, $P_1(t)$,…, $P_k(t)$, $P_l(t)$ соответствуют тому, что в данный момент времени в системе (канале), соответственно, нет срывов и проникновений, один срыв, два срыва связи и т.д. | $\mu = \Delta t_{cp}$<br>Отношение $\lambda/\mu=\alpha$ имеет физический смысл приведенной плотности наступления срывов и поступления проникновений в СДО. Очевидно, что сеть работоспособна, если $\alpha<1$. |
| $P_k(t) = \frac{\alpha^k}{k! \sum_{k=0}^{l} (\alpha^k / k!)}$ | $P_0(t) = 1 \Big/ \sum_{k=0}^{l} \frac{\alpha^k}{k!}$ | $P_1 = \frac{\alpha}{\sum_{k=0}^{l} (\alpha^k / k!)}$ |

| | | |
|---|---|---|
| $P_{\sum ij} = \alpha^N / [\sum_{k=0}^{1} (\alpha^k / k!)]^N$ | Полный срыв связи между i – ми и всеми j – ми абонентами наступит, если пройдет срыв или проникновение у всех N абонентов | $P_{\sum ij} = \alpha^N / [\sum_{k=0}^{1} (\alpha^k / k!)]^N$ |

Относительная надежность канала задается как:

$$y^k_{ij} = 1 - P_1 = 1 - \alpha / [1 + \alpha + \sum_{k=2}^{1} (\alpha^k / k!)]$$

$Y^k_{ij} = 1 - \Delta t^k_{ij} / t^k_{ij}$,. $P1 \approx \alpha / (1 + \alpha)$; $Y^k_{ij} \approx 1 - \alpha / (1 + \alpha) = 1 / (1 + \alpha)$.

$$y_{\sum ij} = 1 - (\alpha / [1 + \alpha + \sum_{k=2}^{1} (\alpha^k / k!)])^{n_{ij}}$$

$y_{\sum ij} = 1 - \Delta t_{\sum ij} / t_{\sum ij}$ ; $P_{\sum ij} \approx P_1^{n}{}_{ij}$; $y_{\sum i} = 1 - \Delta t_{\sum i} / t_{\sum i}$, где $\Delta t_{\sum i} / t_{\sum i} \rightarrow P_{\sum i}$

$\alpha << 1$, $P_{\sum i} = P_1^{Nij} \approx \alpha^{Nij} / (1 + \alpha)^{Nij}$; $y_{\sum i} = 1 - \alpha^{Nij} / (1 + \alpha)^{Ni}$

$y = 1 - \Delta t_{\sum} / t_{\sum} \approx 1 - P_{\sum} = 1 - \alpha^N l^{-\alpha N}$ ; $y^k_{ij}$, $y_{\sum ij}$ и $y_{\sum i}$, ;

$y^k_{ij} = 1 / 1 + \alpha$; $y_{ij} = 1 - \alpha^{nij} / (1 + \alpha)^{nij}$; $y_{\sum i} = 1 - \alpha^{Nij} / (1 + \alpha)^{Nij}$;

$y = 1 - \alpha^N l^{-\alpha N} = 1 - \alpha^N / (1 + \alpha)^N$; $y_{\sum ij} = 1 - (y_{ij}^k)^{nij} \alpha^{nij}$;

$y_{\sum i} = 1 - \alpha^{Nij} (y_{ij}^k)^{Nij}$; $y = 1 - \alpha^N (y_{ij}^k)^N$;

$(1 - y_{\sum ij}) / \alpha^{nij} = (y_{ij}^k)^{nij}$; $(1 - y_{\sum}) / \alpha^{Nij} = (y_{ij}^k)^{Nij}$;

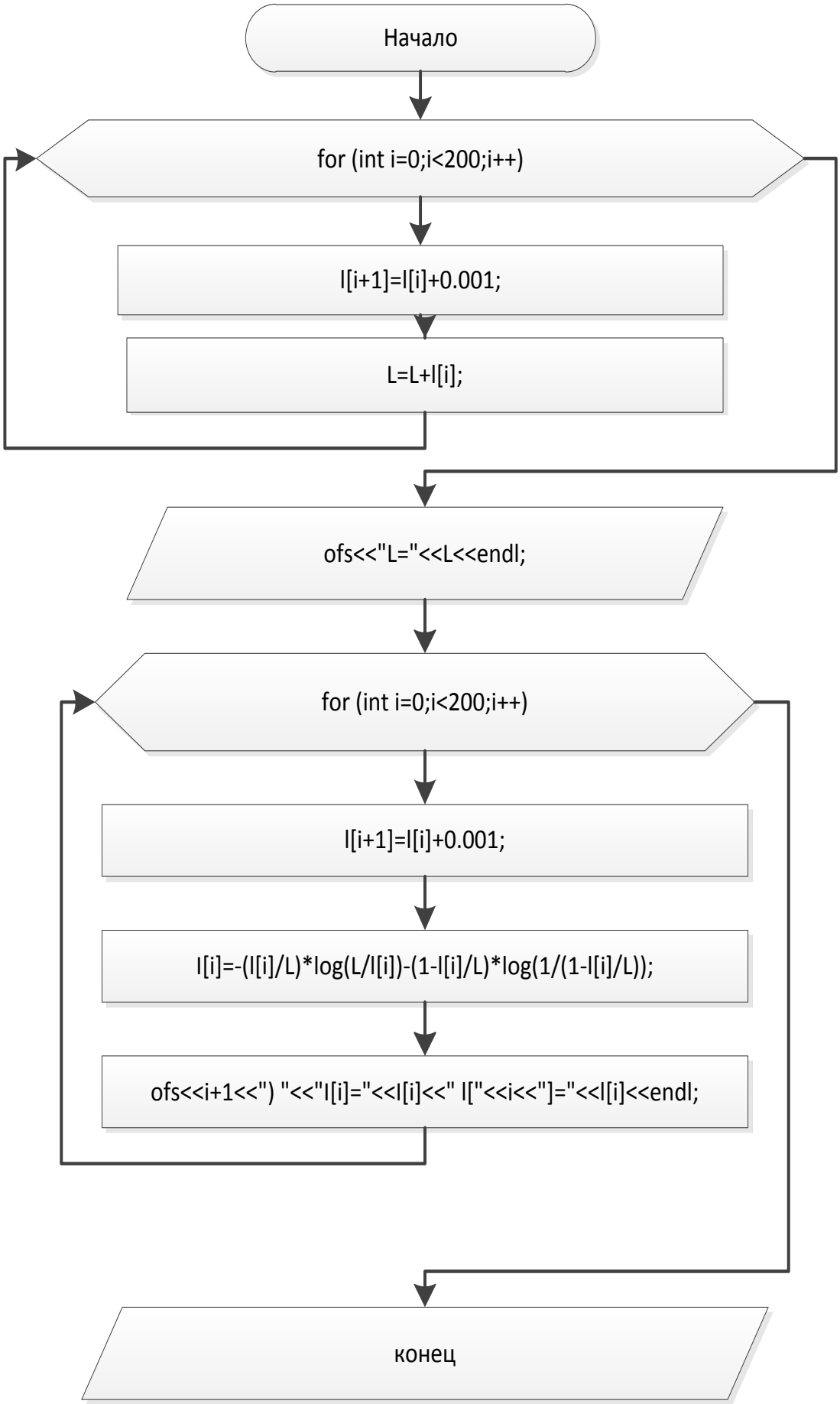
$(1 - y) / \alpha^N = (y_{ij}^k)^N$;

И окончательно получаем

$$\begin{cases} y = 1 - (1 - y_{\sum i})^{N/N_{ij}} \\ y = 1 - (1 - y_{\sum ij})^{N/n_{ij}} \\ y_{\sum i} = 1 - (1 - y_{\sum ij})^{N_{ij}/n_{ij}} \\ y_{\sum ij} = 1 - \alpha^{n_{ij}} (y_{ij}^k)^{n_{ij}} \end{cases}$$

$$\begin{cases} y_{ij}^k = \dfrac{\sqrt[n_{ij}]{1 - y_{\sum ij}}}{\alpha} \\ y_{ij}^k = \dfrac{(1 - y_{\sum i})^{1/N_{ij}}}{\alpha} \\ y_{ij}^k = \dfrac{(1 - y)^{1/N}}{\alpha} \end{cases}$$

Нами, на основании этих методик разработан алгоритм и программа, которые мы использовали при внедрении в ППУ при выборе вариантов проектирования и оценке качества работы СДО [75,98, 99] (см. приложения).


Начало
for (int i=0;i<200;i++)
l[i+1]=l[i]+0.001;
L=L+l[i];
ofs<<"L="<<L<<endl;
for (int i=0;i<200;i++)
l[i+1]=l[i]+0.001;
l[i]=-(l[i]/L)*log(L/l[i])-(1-l[i]/L)*log(1/(1-l[i]/L));
ofs<<i+1<<") "<<"l[i]="<<l[i]<<" l["<<i<<"]="<<l[i]<<endl;
конец

```
#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;
	.....................................................................
	#include "stdafx.h"
#include <stdio.h>
#include <iostream>
#include <string>
#include <cstdlib>
```

L=20.1
1) I[i]=-0.000542665 l[0]=0.001
2) I[i]=-0.00101647 l[1]=0.002
3) I[i]=-0.00146412 l[2]=0.003
4) I[i]=-0.00189498 l[3]=0.004
5) I[i]=-0.00231313 l[4]=0.005
6) I[i]=-0.00272138 l[5]=0.006
7) I[i]=-0.00312118 l[6]=0.007
8) I[i]=-0.00351395 l[7]=0.008
9) I[i]=-0.00390048 l[8]=0.009
10) I[i]=-0.00428147 l[9]=0.01
11) I[i]=-0.00465734 l[10]=0.011
12) I[i]=-0.0050288 l[11]=0.012
13) I[i]=-0.0053961 l[12]=0.013
14) I[i]=-0.00575956 l[13]=0.014
15) I[i]=-0.00611946 l[14]=0.015
16) I[i]=-0.00647603 l[15]=0.016
17) I[i]=-0.00682948 l[16]=0.017
18) I[i]=-0.00718 l[17]=0.018
19) I[i]=-0.00752774 l[18]=0.019
20) I[i]=-0.00787286 l[19]=0.02
21) I[i]=-0.00821547 l[20]=0.021
22) I[i]=-0.00855584 l[21]=0.022
23) I[i]=-0.00889381 l[22]=0.023
24) I[i]=-0.00922961 l[23]=0.024
25) I[i]=-0.00956345 l[24]=0.025
26) I[i]=-0.00989517 l[25]=0.026
27) I[i]=-0.010225 l[26]=0.027
28) I[i]=-0.010553 l[27]=0.028
29) I[i]=-0.0108792 l[28]=0.029
30) I[i]=-0.0112038 l[29]=0.03
31) I[i]=-0.0115267 l[30]=0.031
32) I[i]=-0.0118478 l[31]=0.032
33) I[i]=-0.0121675 l[32]=0.033
34) I[i]=-0.0124858 l[33]=0.034
35) I[i]=-0.0128024 l[34]=0.035
36) I[i]=-0.0131177 l[35]=0.036
37) I[i]=-0.0134316 l[36]=0.037
38) I[i]=-0.0137442 l[37]=0.038
39) I[i]=-0.0140554 l[38]=0.039
40) I[i]=-0.0143654 l[39]=0.04
Остальные данные приведены в приложении 3.3.1.

## 3.4. Эффективность информационного канала СДО с учетом защитных мероприятий

В ТС СДО эффективность обеспечивается из-за уменьшения расходов на эксплуатационные потери из-за устранения ПИП и уменьшения проникновений, при этом приведенные затраты [74,75]

$П_{изн} > П_{изс}$ ; $П_э = \varepsilon + E (П_{из} + К_м + \ldots)$ . [ 87,89]

$$\varepsilon = С_э + С_р + С_{пр} + С_г + С_{кач} .$$

Все эти параметры укажем в табл.3.4.1.

Таблица 3.4.1. Составляющие эффективности и условия обеспечения

| Составляющие | Содержание | Обеспечение |
|---|---|---|
| $С_э$ | эксплуатационные расходы на энергию, зарплату обычному личному составу | Администрация |
| $С_р$ | расходы на ремонт с учетом замененных деталей и зарплаты личному составу повышенной квалификации | Проект, заказчик |
| $С_{пр}$ | расходы из-за временной неработоспособности (простоя) СДО, которые отрицательно отражаются на обслуживаемых процессах | администрация, заказчик |
| $С_г$ | стоимость потери какой – либо обслуживаемой технической системы или нарушения технологического процесса из-за отказа СДО или проникновения в нее | Проект, администрация, |
| $С_{кач}$ | составляющая , зависящая от качества СДО, а именно от одного или ряда определяющих параметров | Проект, администрация, заказчик |

$C_э(\theta, S, G)$; $C_р(\theta, H, S)$; $C_{пр}(\theta, H, V)$; $C_г(H, M)$; $C_{кач}(P, Z)$ .

Таблица 3.4.2. Составляющие затрат

| Составляющие | Содержание | Обеспечение |
|---|---|---|
| $\theta$ | время эксплуатации | Администрация |
| S | величина, зависящая от сложности СДО | Проект, заказчик |
| G | величина, определяемая энергетическими показателями СДО | Проект, администрация |
| H | величина, определяемая одной или совокупностью характеристик надежности СДО | Проект, заказчик |
| V | объем обслуживания СДО с помощью РЭС (часть информационной и учебной продукции) | Проект, администрация |
| M | стоимость материальных ценностей, обслуживаемых СДО | Администрация |
| P | значения определяющих параметров | Проект, заказчик |
| Z | изменение стоимости других систем при внедрении СДО (с защитными мероприятиями) | Проект, |

$П_{э\ тс\text{-}зм} = \varepsilon_{тс\text{-}зм} + E(П_{изтс} + П_{изку} + К_{мрэс} + К_{мзм} + \ldots)$ ,

$\varepsilon_{тс\text{-}зм} = c_{этс} + c_{эзм} + c'_{р} + c'_{пр} + c'_{г} + c'_{кач}$ .

$Э = П_{э\ тс} - П_{э\ тс\text{-}зм} = -c_{эзм} + (c'_{р} - c'_{р}) + (c_{пр} - c'_{пр}) + (c_{кач} - c'_{кач}) + E(-П_{иззм} - К_{мзм})$.

$C_{ПР} \supseteq \theta k(H)(c_э + c_р)2$ ; $C_Г \supseteq k(H)C_{\text{ТЕХН.КОМПЛЕКСА}}$ ,

Или $k(H) = 1 - P_{нФ}$.

$C_{пр} = C_п \tau_b \theta_0 (1 - e^{-\theta/\theta_0}) / T_0$ ; $C_г = C_{ги}(1 - К_г)$ .

При введении в СДО ЗМ, ее коэффициент готовности повышается до $К_{гку}$, а общая стоимость

$$С_{ку}= С_{кку} + С_{ркy} + С_{прку} + С_{гку}; \quad С_{кку} =С_к + С'_{кку}$$

$$С'_{кку} = A D^l / [(1-B)^k К_г /К_{гу}) + t \log_c [ A / (1-B)^k К_г /К_{гу} ]. \quad [74]$$

Таблица3.4.3. Составляющие стоимости ЗМ

| Составляющие | Содержание | Обеспечение |
|---|---|---|
| B | критерий объективности контроля | Заказчик |
| D | коэффициент, определяемый в зависимости от вида ЗМ, выполняемых им функций (контроль работоспособности, отыскание неисправностей и проникновений, прогнозирование) | Проект, заказчик |
| l | коэффициент, зависящий от сложности контроля определяющих параметров, от степени автоматизации | Проект |
| k | коэффициент, зависящий от способа обработки информации с датчиков | Проект, заказчик |
| t | коэффициент, зависящий от ЗМ, от вида индикации | Проект, администра-ция, |
| c | определяется ограничениями по стоимости, массе и габаритам, предъявляемыми к СДО | Проект, администрация, заказчик |

Все остальные составляющие соотношения также изменяются, так как обычно

$$К_{гку} \supseteq К_г; \qquad \tau_{вку} < \tau_в; \qquad С_{раб\ ЗМ} < С_{раб}.$$

$К_{гку} > К_г$ при $С_{ЗМ} = С$ или $К_{гку} = К_г$ при $С_{ЗМ} < С$ [96].

Эти соотношения для защищенной СДО мы преобразовали для условий Палестины и использовали при внедрении в ППУ, где они показали очень хорошие результаты (см. Приложения).

### 3.5. Выводы по главе 3

1. Приведенные методики решают проблемы экономического обоснования мероприятий по защите от несанкционированного доступа для каждой конкретной СДО в зависимости от задач стоящих перед ними в каждом отдельном случае.
2. Смоделирован для этих случаев информационный канал и проверена его адекватность.
3. Показано, что для СДО в конечном итоге важна эффективность сети связи в зависимости от срывов (в том числе и от проникновений в нее).
4. Разработанные нами расчетные методики позволяют обоснованно оценить эффективность с учетом ограничений.

# ГЛАВА 4. ЗАЩИТА ТЕЛЕКОММУНИКАЦИЙ СДО ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ В ПАЛЕСТИНЕ И МЕТОДИКИ ОЦЕНКИ ЭФФЕКТИВНОСТИ ОТ ЭТОГО

В Палестине радиосистемы для защиты информации стали актуальными за последние годы потому, что при несанкционированном добывании информации используется широкий арсенал технических средств, из которых в основном малогабаритные отражают одно из направлений в развитии современных разведывательных технологий. Выполняемые в портативном, миниатюрном и сверхминиатюрном видах эти средства аккумулируют в себе новейшие научные, технические и технологические достижения электроники, акустики, оптики, радиотехники и других наук. Такие средства находят широкое применение как в деятельности правоохранительных органов, так и иностранных технических разведок, в подпольном информационном обеспечении незаконных экономических, финансовых и криминальных организаций. В условиях рыночной экономики появление значительного числа конкурирующих между собой различных структур естественным образом создало определенное пространство, на котором применение подобных устройств технической разведки для добывания информации различной значимости является наиболее вероятным.

Для решения поставленных целей необходимо[14,74,75,90] табл.4.1:

Таблица 4.1. Цели защиты СДО в Палестине

| Цели | обеспечение |
|---|---|
| разработать методики, технико–экономического обоснования мероприятий по защите от | Проект, заказчик |

| | |
|---|---|
| несанкционированного доступа и оценить эффективность информационного канала с учетом защитных мероприятий для конкретных телекоммуникаций СДО Палестины и и аналогичных сетей России | |
| разработать методики, средства защиты и оценивать показатели надежности и уровень технического состояния системы связи и передачи информации, применительно к конкретным предприятиям Палестины и к аналогичным им в России | Проект |
| провести моделирование, экспериментальные исследования и сделать экономические оценки с разработкой рекомендации по защите корпоративной информации в Палестине | Проект |

Применительно к Палестине и к внедрениям в России это оригинальные разработки автора.

## 4.1. Математическое моделирование процессов проникновения в канал и защиты радиосистем от несанкционированного доступа

### 4.1.1. Информационная надежность защищаемого канала

Нарушение работоспособности характеризуется невыполнением одного или нескольких условий, характерных для исправного канала. Чаще всего оценивают нарушение работоспособности по выявлению внезапных отказов, недопустимого изменения какого-либо выходного параметра (постепенные отказы) или проникновения в канал. С точки зрения надежности эти нарушения идентичны[74,75].

При такой постановке задачи на аппаратуру контроля возлагается не только фиксация наступивших отказов, оценка уровня технического состояния и прогнозирование возможного последующего ухудшения состояния отдельных параметров или канала в целом, но и обнаружение проникновения в него. Решение поставленной задачи требует, прежде всего, установления параметров, которые должны контролироваться, а для этого необходимо получить количественное соотношение уровня технического состояния канала по постепенным отказам. Этот вид нарушений наиболее общий в системном плане и с его помощью можно учесть остальные нарушения. Используем последовательную структурную схему надежности, но учитываем, что выходные параметры различных блоков неодинаково влияют на выходные параметры системы в целом. Поэтому при изучении влияния уходов выходных параметров блоков этим параметрам должны приписываться неодинаковые веса. При изучении влияния постепенных отказов канала длительного использования может с успехом использоваться частотный критерий надежности (спектральный метод). При этом уход величины выходного параметра за допустимые пределы можно рассматривать как отказ аналогично внезапному отказу элемента в системе.

### 4.1.2. Уровень технического состояния канала с учетом проникновений

При оценке уровня технического состояния используем следующие допущения (в предположении правильной организации эксплуатации)[74,75]:

- имеется $N$ выходных параметров канала $j$, которые равнозначны (одинаково влияют на надежность);

- аппаратура состоит из $M$ блоков $i$, каждый из которых имеет $L_i$ выходных параметров $k$;

- предполагаются малые изменения значений параметров;

- все блоки эксплуатируются в одинаковых условиях;

- не учитываются корреляционные зависимости между *ik*-ми параметрами.

В силу указанных допущений уровень технического состояния канала по проникновениям НСД можно оценить выражением[75]

$$P \approx \prod_{i=1}^{M} \prod_{k=1}^{L_i} P_{ik} = \prod_{i=1} \prod_{k=1} (1 - Q_{ik}).$$

где $P_{ik} \approx (1 - Q_{ik})$ – вероятность безотказной работы $k$-го выходного параметра $i$-го блока (вероятность нахождения значения параметра в допуске) с учетом его важности (влияния на выходные параметры канала).

Можно предложить для оценки $Q_{ik}$ соотношение[75]

$$Q_{ik} = h_{ik} q_{ik}.$$

Здесь $h_{ik}$ – относительный «вес» («важность») $ik$-го параметра (влияние его в целом на все выходные параметры канала):

$$\sum_{i=1}^{M} \sum_{k=1}^{L} h_{ik} = 1;\ h_{ik} > 0;$$

$q_{ik}$ – вероятность постепенного отказа $k$-го параметра $i$-го блока, которая может быть определена методами, изложенными в [75].

$$h_{ik} = \frac{\sum_{j=1}^{N} X_{jik}}{\sum_{j=1}^{N} \sum_{ij=1}^{M} \sum_{k=1}^{N} X_{jik}} \qquad (4.1.6)$$

В предложенной оценке хорошо учитывается структура канала. Она может применяться для тех каналов, для которых возможно определение $X_{ijk}$ расчетными или экспериментальными методами. При этом учитывается влияние параметров на надежность или эффективность канала.

### 4.1.3. Зависимость изменения выходного параметра канала от изменения параметров элементов

Для выявления зависимости изменения выходных параметров (уровня технического состояния) канала от изменения параметров трактов, блоков, каскадов (и элементов) и от проникновений выразим

$$\delta A = f(\delta x_1, \delta x_2, \dots, \delta x_n).$$

При этом пользуемся предположением о различной степени влияния изменения параметра каждого элемента (под элементом понимаем здесь и далее тракт, блок, каскад) на изменение выходного параметра. Такой подход наиболее целесообразен и в условиях производства, и в условиях эксплуатации[75].

Обычно для оценки влияния параметра $x$ на стабильность выходного параметра $A$ используют чувствительность или, по другому, коэффициент влияния.

Определение коэффициентов влияния может быть расчетным и экспериментальным[75]. В тех случаях, когда трудно или невозможно применять расчетные методы, используют экспериментальные в предположении, что, если дать отклонение от номинала одного из параметров $\Delta x_i/x_i \neq 0$ при постоянных остальных, то отклонение выходного параметра будет определяться лишь этим отклонением.

По опыту наших внедрений и из указаний, приведенных в [75] можно указать, что наиболее приемлемым следует считать граничные испытания.

При выборе параметров граничных испытаний необходимо выполнение следующих основных требований (табл.4.1.3.1):

Таблица 4.1.3.1. Выбор параметров для граничных испытаний

| Требование, обеспеченное в сети/структуре | Соблюдение/соответствие |
|---|---|
| влияние параметра на выходные характеристики схемы должно быть определяющим | Хорошее |
| зависимость его от изменения внешних условий и параметров элементов должна быть минимальной | среднее |
| пределы изменения параметра при проведении испытаний должны быть достаточно широкими | плохое |
| изменение граничного параметра в указанных пределах не должно приводить к существенному изменению параметров элементов | Хорошее |

В общем случае коэффициент влияния определяется по формуле[75]

$$Xx_i = \frac{\delta A(1-\delta Z/\delta Z_o)}{\delta x_i},$$

Эти методики могут применяться при определении коэффициентов влияния в сетях, в каналах, для каскадов, блоков и трактов. В этом мы убедились при внедрении в Палестинском политехническом университете.

При компьютерных технологиях применение методик очень эффективно.

### 4.1.4. Выигрыш во времени использования канала за счет уменьшения числа ошибок при отыскании проникновений и защите канала

При диагностике канала выигрыш во времени использования получается не только за счет уменьшения среднего времени на отыскание проникновений и расстроенных параметров, но и за счет уменьшения повторных информационных потоков (ПИП)[74,75]. Под ПИП понимается число дополнительных связей при защите канала.

Причиной их появления чаще всего являются или недостаточная квалификация обслуживающего персонала, или недостаточная защита. Оценим выигрыш во времени использования за счет уменьшения его на отыскание проникновений. Полезно также оценить и выигрыш за счет уменьшения числа ПИП в предположении, что контролируемые параметры (элементы) ограждены от ошибок.

Произведена оценка выигрыша для частного случая, когда полное среднее время использования τ определяется соотношением

$$\tau = \tau_b^{'} + \tau_{\text{пн}}, ,$$

$$\tau_b = \tau_b^{''} + \tau_{\text{пн}},$$

Таблица 4.1.4.1. Временные соотношения

| Значение | Наименование | соответствие |
|---|---|---|
| $\tau_b^{'}$ | среднее время использования, определенное без учета ПИП | Проект, статистика |
| $\tau_{\text{пн}}$ | среднее время использования за счет появления ПИП | Проект |
| $\tau_b$ | среднее время использования, определяемое из статистических данных | Проект, статистика |

| | | |
|---|---|---|
| $\tau_b''$ | среднее время восстановления без учета ПИП, в отличие от $\tau_b'$ – неизвестное | Проект |
| $P_i$ | вероятность отказа $i$-го элемента | статистика |
| $P_{\text{пн}i}$ | вероятность возникновения ПИП при защите, связанной с проникновением в зоне $i$-го элемента | Проект, статистика |
| $P_{\text{по}i}$ | вероятность ПИП при отыскании проникновения в зоне $i$-го элемента | Проект, статистика |
| $P_{\text{пу}i}$ | вероятность ПИП при устранении проникновения в зону $i$-го элемента | Проект, статистика |

$$\tau_{\text{пн}} = \sum_{i\in\Omega} P_i P_{\text{пн}\,i}\,\tau_{\text{пн}\,i},$$

$$P_{\text{пн}\,i} = P_{\text{по}i} + P_{\text{пу}i},$$

$$\tau_{\text{пн АОН}} = \sum_{i\in\Omega} P_i P_{\text{пн}\,i}\,\tau_{\text{пн}i} + \sum_{i\in\Omega} P_i P_{\text{пу}\,i}\,\tau_{\text{пн}\,i},$$

$$\overline{w} \cup w = \Omega;\ \overline{w} \cap w = \varnothing\ .$$

Приведем используемые значения в табл.4.1.4.2.[74,75]

Таблица 4.1.4.2. Составляющие выигрыша во времени использования

| Значение | Наименование | соответствие |
|---|---|---|
| $w$ | подмножество диагностируемых элементов | статистика |
| $\tau_{\text{пн}i}$ | время, потребное на отыскание и устранение ПИП, связанных с отказом $i$-го элемента | Проект, статистика |
| $\Omega$ | множество элементов (параметров) канала | заказчик, статистика |

Выигрыш во времени использования при этом равен

$$\Delta\,\tau_{\text{пн АМЗК}} = \tau_{\text{пн}} - \tau_{\text{пнАМЗК}}\,.\quad \tau_{\text{в АМЗК}} = \tau_{\text{в}} - \Delta\tau_{\text{пн АМЗК}}\,,$$

Теперь можем определить коэффициент проникновений $К_{пн}$ [75]

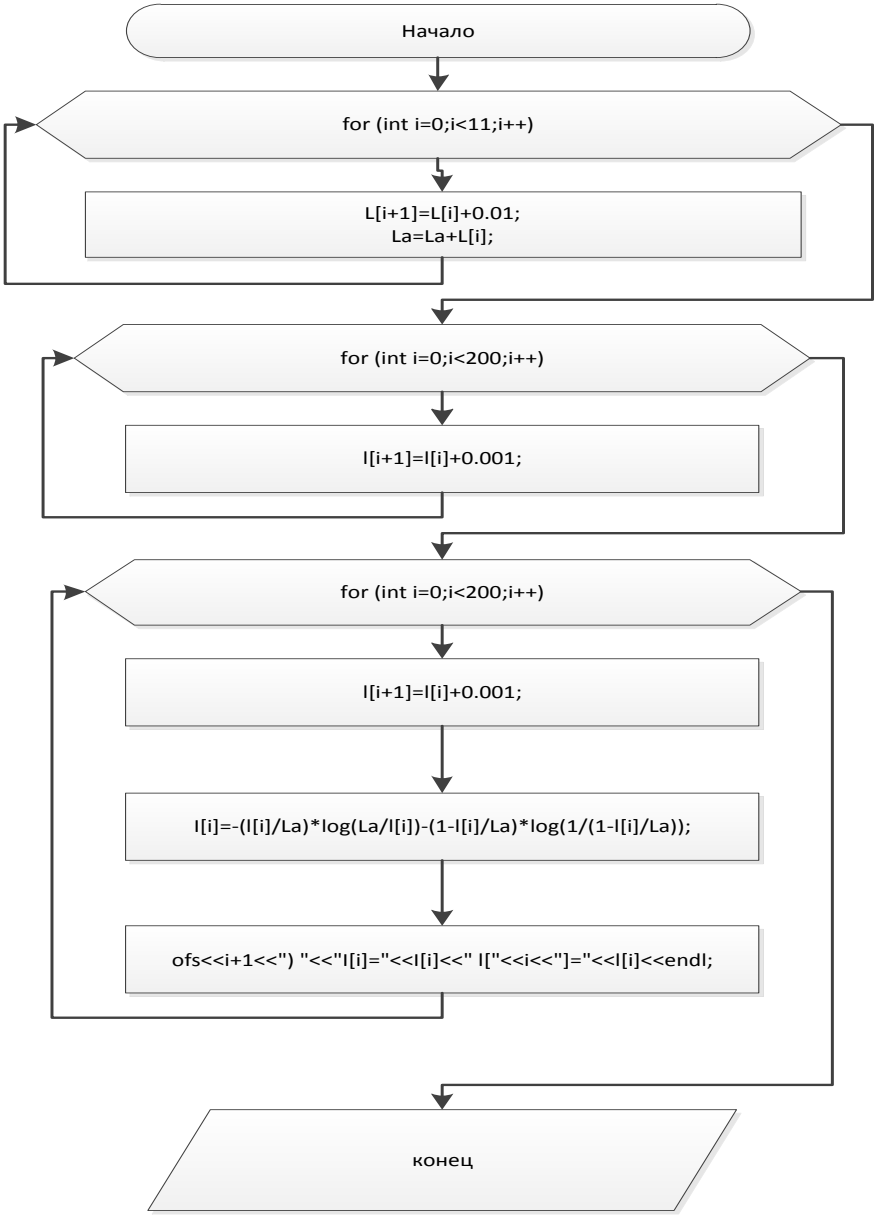
$$К_{пн} = 1 + \frac{P_{п}}{1 - P_{п}}\,.$$

$$К_{пнАМЗК} = 1 + \frac{P_{АМЗК}P_{пу} + (1\text{-}P_{АМЗК})P_{п}}{1 - P_{АМЗК}P_{пу} - (1 - P_{АМЗК})\,P_{п}}\,,\qquad P_{АМЗК} = \frac{\sum\limits_{i\in W}\lambda_i}{\Lambda}.$$

Находим выигрыш во времени для канала, сети, сервера от проникновений и от ПИП [75]

$$\Delta\,\tau_{\text{пн АМЗК}} = \tau_{\text{в}}(К_{пн} - К_{\text{пн АМЗК}})\,.$$

Нами разработан, алгоритм и программа для этих расчетов.




```
#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;
	.....................................................................
	#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[202];
float I[202];
float L[11];
float La=0;
l[0]=0.001;
```

```
L[0]=0.9;
std::ofstream ofs("tablica.txt");
for (int i=0;i<11;i++)
{
L[i+1]=L[i]+0.01;
La=La+L[i];
for (int i=0;i<200;i++)
l[i+1]=l[i]+0.001;
for (int i=0;i<200;i++)
l[i+1]=l[i]+0.001;
I[i]=-(l[i]/La)*log(La/l[i])-(1-l[i]/La)*log(1/(1-l[i]/La));
ofs<<i+1<<") "<<"I[i]="<<I[i]<<" l["<<i<<"]="<<l[i]<<endl;
}
system ("pause");
ofs.close();
return 0;
```

**.....**

```
#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[202];
float I[202];
float L=0;
l[0]=0.001;
std::ofstream ofs("tablica.txt");
for (int i=0;i<200;i++)
{
l[i+1]=l[i]+0.001;
L=L+l[i];
```

```
}
ofs<<"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));
ofs<<i+1<<") "<<"I[i]="<<I[i]<<" l["<<i<<"]="<<l[i]<<endl;
system ("pause");
ofs.close();
return 0;
```

С помощью этой программы мы рассчитали выигрыш при устранении ПИП в сети СДО ППУ и получили хорошие результаты (см. Приложения).

### 4.2. Улучшение информационной защиты радиосистем СДО

Для приближенных расчетов по информативным признакам предлагаем использовать методику предложенную Галкиным А.П.[74,75].

Решение этой задачи возможно при допущениях соответствующим особенностям СДО Палестины (см. главу 1 и приложения).

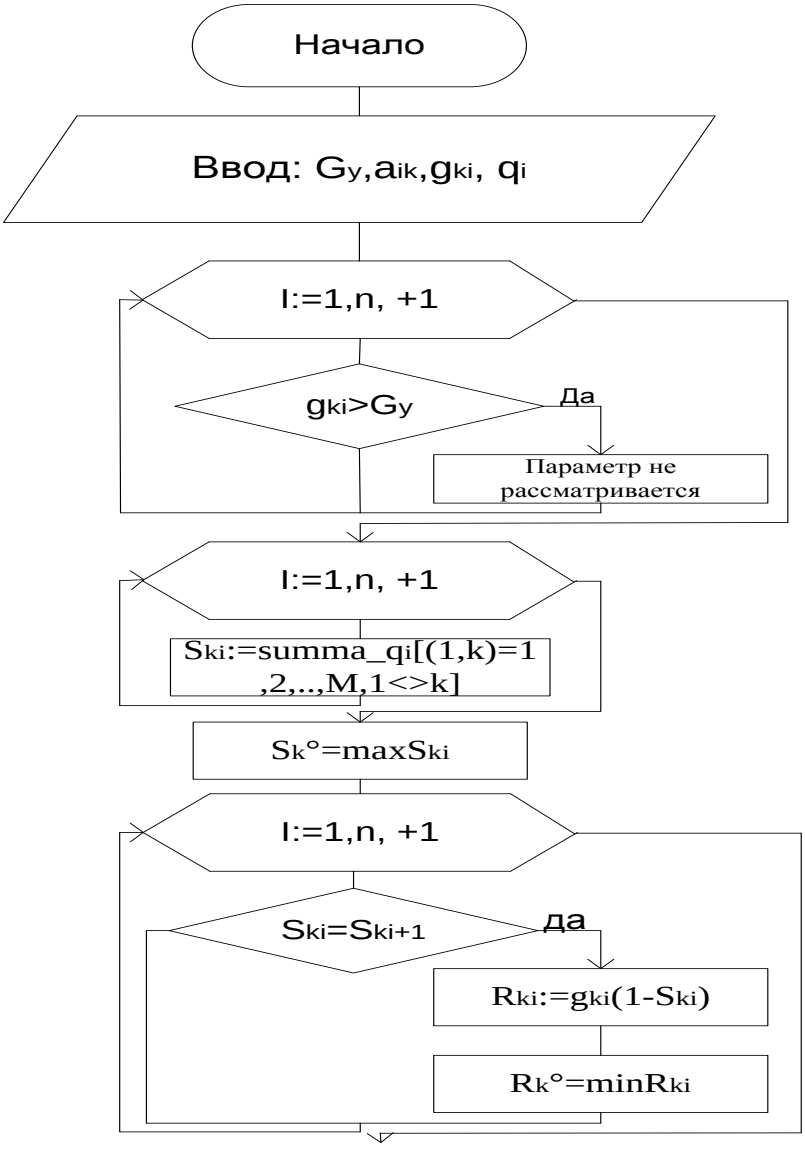
$$B_{\omega} = \max_{\omega \in \Omega} \{B / g_s \le G_s;\ s = 1,2\ldots\},$$

Значения используемые в расчетах по этой методике располагаем в табл.4.2.1.

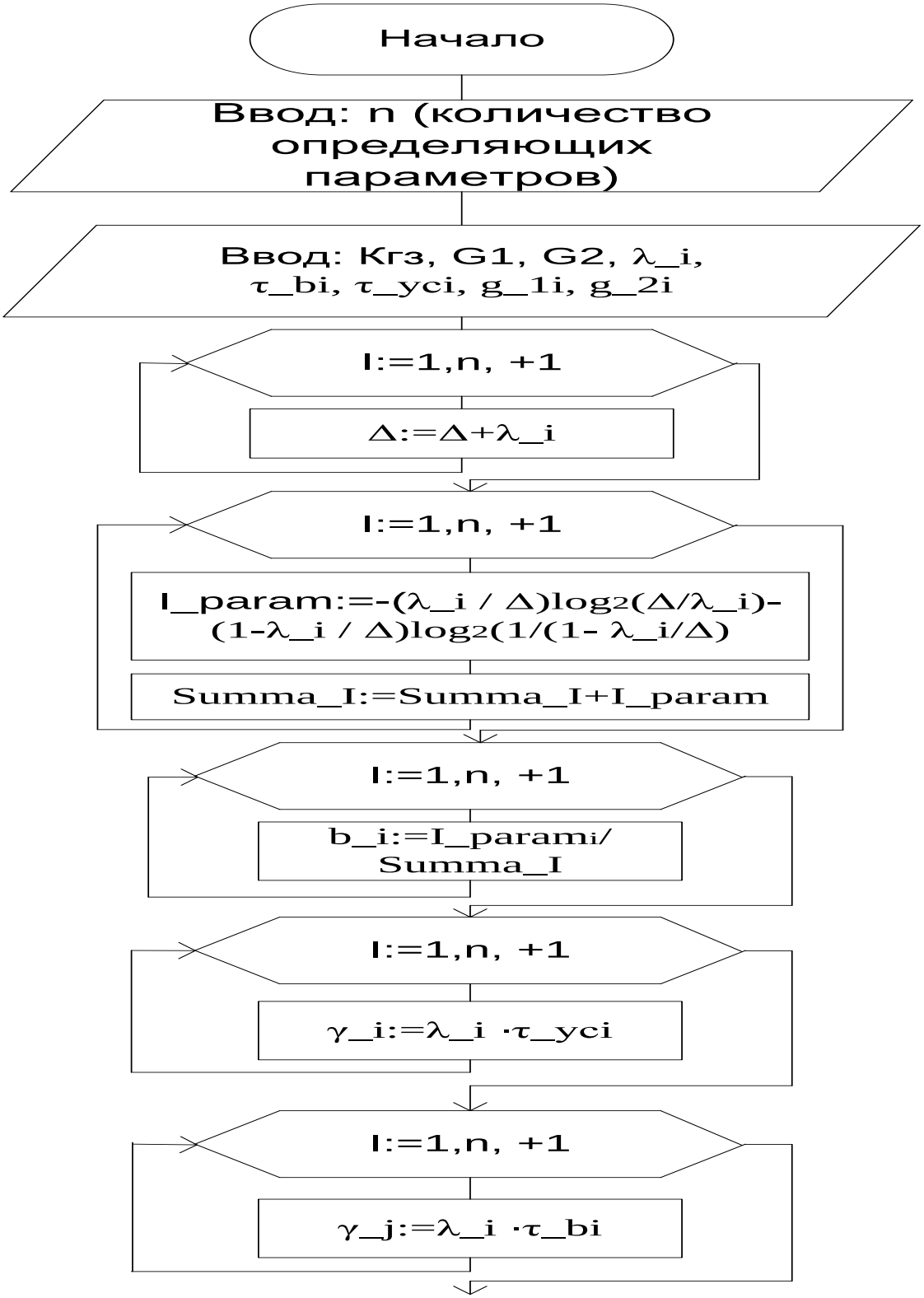
Таблица 4.2.1. Значения максимизации

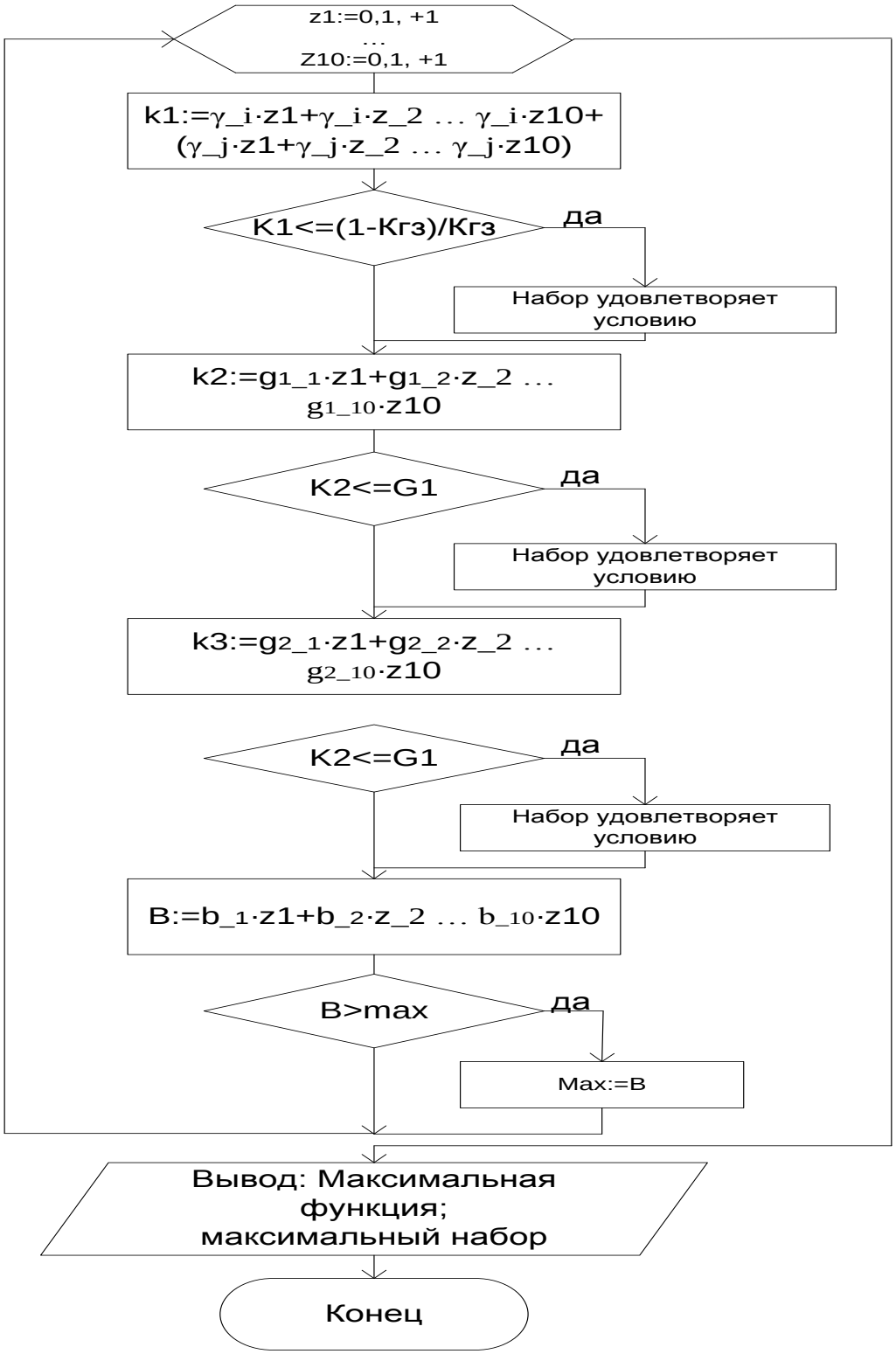
| Значение | Соответствие | Назначение |
|---|---|---|
| $g_s$ | достигнутое значение по *s*-му ограничению | проект |
| $G_s$ | ограничение на выбор состава контролируемых параметров | заказчик |
| Gy | ограничение на проведение контроля | проект |
| $g_k$ | затраты на контроль параметра | проект |
| $a_{ik}$ | двоичная матрица объектов контроля | проект |
| $q_i$ | априорные вероятности отказа i-того элемента | заказчик |
| $S_k$ | ненадежность k-го параметра (πk) | заказчик |

| | | |
|---|---|---|
| $P_{i(k)}$ | вероятность безотказной работы | заказчик |
| $\pi_k$ | параметр сети СДО | проект |
| $\pi^\circ_k$ | оптимальный параметр | заказчик |
| $G_{1,2}$ | ограничение контролируемых параметров | проект |
| $g_{1,2}$ | достигнутое значение по s-му ограничению | проект |
| $\lambda_i$ | интенсивность проникновений в i-тый параметр | проект |
| $\Delta$ | интенсивность проникновений в канал | заказчик |
| $\tau_{bi}$ | время восстановления i-го элемента | заказчик |
| $\tau_{yci}$ | время устранения неисправности i-го элемента | заказчик |



Выбор контролируемых параметров по максимальным значениям.




z1:=0,1, +1
...
Z10:=0,1, +1
k1:=γ_i·z1+γ_i·z_2 ... γ_i·z10+
(γ_j·z1+γ_j·z_2 ... γ_j·z10)
K1<=(1-Кгз)/Кгз
да
Набор удовлетворяет условию
k2:=g1_1·z1+g1_2·z_2 ...
g1_10·z10
K2<=G1
да
Набор удовлетворяет условию
k3:=g2_1·z1+g2_2·z_2 ...
g2_10·z10
K2<=G1
да
Набор удовлетворяет условию
B:=b_1·z1+b_2·z_2 ... b_10·z10
B>max
да
Max:=B
Вывод: Максимальная функция;
максимальный набор
Конец

```
#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;
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.

//////////////////////////////////////////////////////////////////////////// // 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 #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>

Применяем в качестве максимизируемой функции критерия объективности контроля в виде[75]

$$b_i = \frac{I_i}{\sum_{i\in\omega} I_i} \qquad B_\omega = \sum_{i\in\omega} b_i$$

$$I_i = -\frac{\lambda_i}{\Lambda}\log_2\frac{\Lambda}{\lambda_i} - \left(1-\frac{\lambda_i}{\Lambda}\right)\log_2\frac{1}{\left(1-\frac{\lambda_i}{\Lambda}\right)} \qquad \lambda_i << \Lambda ;$$

$$\tau_{от\,i} + \tau_{ус\,i} = \tau_{в\,I}; \tau_{от\,ку\,i} << \tau_{ус\,i}.$$

Эти расчетные соотношения и разработанный нами алгоритм, сделанные нами в Палестинском политехническом университете и на телекоммуникационной сети завода «Электроприбор» (г. Москва), которая аналогична по своей логике и структуре сетям СДО Палестины показали хорошие результаты и были с благодарностью приняты персоналом, занятым на обслуживании сетей.

Для компьютерного определения наилучшего времени между проведением диагностики информационного канала разработаем подходы [74,75] значения составляющих приведем в табл.4.2.2.

$$K_г = \frac{T_о}{T_о + \tau_в + P_{фк}\ T_{фк}/2} \quad \frac{T_{фк}}{T_{фк} + \tau_{фк}},$$

Таблица 4.2.2. Составляющие для диагностики

| Значение | Соответствие | Назначение |
|---|---|---|
| $T_о$ | среднее время работы канала между проникновениями | статистика |
| $\tau_в$ | среднее время существования проникновения ($\tau в = \tau от + \tau ус$) | статистика |
| $T_{фк}$ | среднее время между проведением диагностики | заказчик, статистика |
| $\tau_{фк}$ | среднее время проведения диагностики | заказчик, проект |

Максимальный коэффициент готовности получается при времени между проведением диагностики [75]

$$T_{фк} = \sqrt{\frac{2\tau_{фк}(\tau_о + \tau_в)}{P_{фк}}}.$$

Разработанный нами подход показал очень хорошие результаты при практическом использовании и при внедрении в Палестинском политехническом университете. Он оказался понятным и доступным для всех сетевых администраторов. Они приняли его для неуклонного использования (см. приложения).

## 4.3.Обеспечение информационной безопасности компонентов информационно-образовательной среды в условиях Палестины

### 4.3.1. Архитектура безопасности СДО предлагаемая для условий Палестины

Проблемы безопасности в СДО можно разделить на следующие направления[75] табл.4.3.1:

Таблица 4.3.1. Технологические группы безопасности в СДО

| Технологическая операция | Пользователи | Ответственный |
|---|---|---|
| Аутентификация | Тьюторы, студенты, администрация | администрация, администратор сети |
| Авторизация | Тьюторы, студенты | администратор сети |
| Аудит | Тьюторы, студенты, администрация, | администрация, администратор сети |
| конфиденциальность | Тьюторы, студенты, администрация, | администратор сети |
| Доступность | Тьюторы, студенты, администрация, | администрация, администратор сети |
| Целостность | Тьюторы, студенты, администрация, администратор сети | администрация, администратор сети |

В таблице 4.3.2 представлены технологии Microsoft, обеспечивающие защиту приложения по каждому из основных аспектов защиты.

Таблица 4.3.2. Технологии Microsoft, обеспечивающие защиту Интернет-приложений

| Категория | Технологии |
|---|---|
| Аутентификация | Kerberos Запрос/ответ<br>Windows |
| Авторизация | Списки контроля доступа<br>Разрешения SQL Server<br>Разрешения IIS |
| Целостность | Брандмауэр |
| Аудит | Журналы системы защиты. Журналы IIS<br>Регистрационные файлы и трассировки SQL Server |
| Доступность | Журналы<br>аудита |

На рис. 4.3.2.1 представлена модель Интернет-приложения, построенная с учетом реализации описанных категорий безопасности с использованием технологий Microsoft [71].

### 4.3.2. Обеспечение безопасности модулей информационно-образовательной среды

В разработанной ИОС безопасность Web-модулей обеспечивается в соответствии с выше описанной архитектуры безопасности Интернет-приложений.

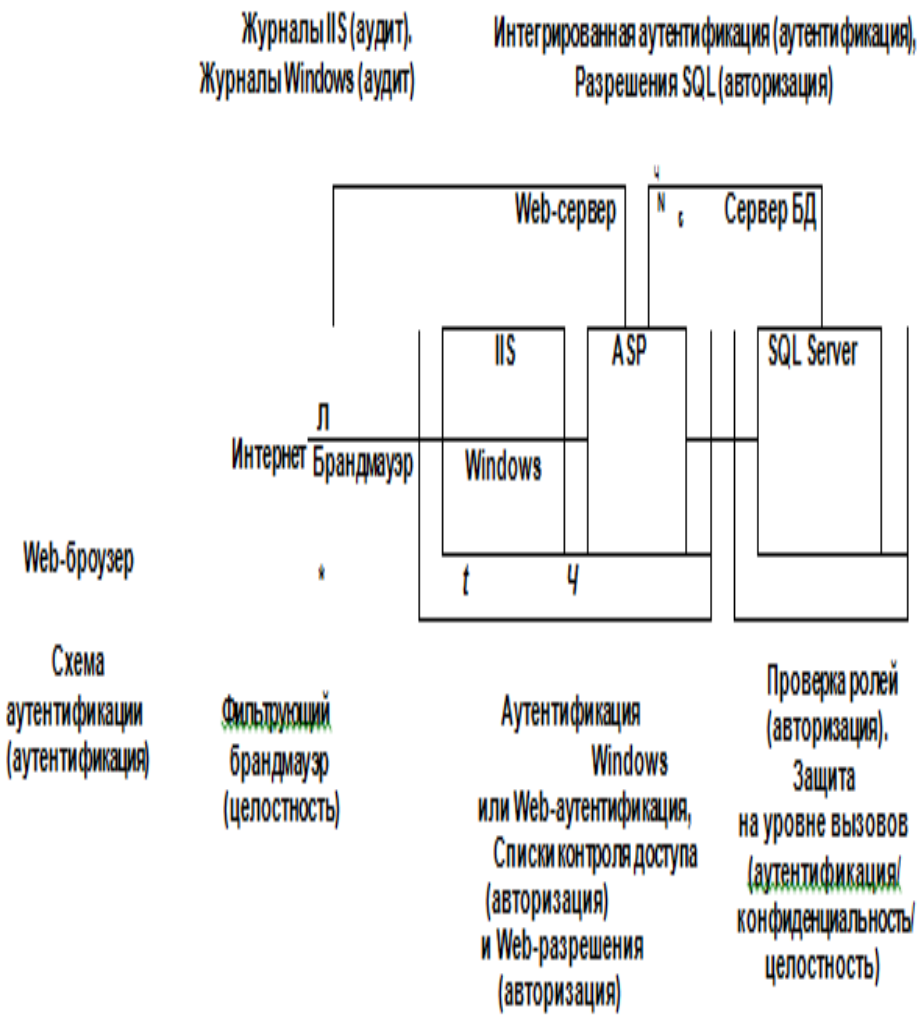



Рис. 4.3.2.1. Безопасность СДО для условий Палестины

Основные принципы аутентификации и авторизации внешних пользователей, применяемые в Web-модулях ИОС (табл.4.3.2):

Таблица 4.3.2. Основные права пользователей в СДО

| Пользователи и их права | Ответственный |
|---|---|
| Анонимный доступ к ASP-страницам приложения | администрация, администратор сети |
| Права пользователей проверяются в базе данных SQL Server | администратор сети |

| | |
|---|---|
| Для каждого пользователя создается индивидуальный ASP-сеанс, который несет информацию о правах пользователя и определяет доступ к соответствующим функциям ASP-модулей | Тьюторы, студенты, администратор сети |
| Web-приложение соединяется с базой данных под идентификатором ASP-процесса | Тьюторы, администратор сети |
| Единственная пользовательская роль используется в базе данных SQL Server для авторизации | администратор сети |

## 4.4. Выводы по главе 4:

1. Разработаны методики обоснования мероприятий по защите от несанкционированного доступа и оценена эффективность информационного канала с учетом защитных мероприятий для конкретных телекоммуникаций в Палестинском политехническом университете.
2. Разработаны методики, средства защиты и оценены показатели надежности и уровень технического состояния системы связи и передачи информации, применительно к конкретным предприятиям.
3. Проведено моделирование, экспериментальные исследования и сделаны оценки с разработкой рекомендаций по защите корпоративной информации в сети в Палестинском политехническом университете и в аналогичных сетям СДО Палестины.
4. Разработаны методики выбора контролируемых параметров систем для достижения заданных результатов.
5. При решении поставленных задач было использован аппарат математического анализа, теории вероятностей и случайных процессов, теории надежности и программирования.

# 5. ЗАКЛЮЧЕНИЕ

**Основные результаты диссертационной работы:**

1. Разработана методика оценки эффективности мероприятий по защите от несанкционированного доступа и определена технико-экономическая оценка адекватности моделирования информационного канала СДО.

2. Предложена зависимость эффективности сети связи от срывов и оценена эффективность информационного канала с учетом защитных мероприятий для целей улучшения работы СДО.

3. Приведен математический анализ эффективности защитных мероприятий, который может быть использован в методиках по защите информации.

4. Разработаны методики и средства защиты системы связи и передачи информации, применительно к наиболее распространенным СДО, оценены показатели надежности и уровень технического состояния защищаемого канала и обосновано применение теории надежности для построения модели канала со срывами связи и проникновениями в него.

5. Разработаны принципы построения систем защиты информации в современных системах передачи и обработки данных, методика защиты информации в системе корпоративной связи СДО.

6. Предложена методика выбора контролируемых параметров по максимальным значениям (с учетом защиты канала), разработан выбор контролируемых параметров по заданному коэффициенту готовности и проведен выбор контролируемых параметров по максимальному значению вероятности безотказной работы после проведения диагностики с оценкой оптимального времени между проведением функциональных проверок информационного канала; внедрение методики позволило увеличить эффективность защиты на 70-90%.

8. Разработаны методики и алгоритмы для синтеза маршрутизаторов в сети СДО и их минимизация на этапе проектирования применительно к условиям Палестины; они позволили сократить время проектирования в 3 раза, а число маршрутизаторов сократить в 2 раза.

9. Программные продукты по защите информации в каналах и методики реализованы в Палестинском политехническом университета ППУ, (Палестина), НПО «РИК» (г. Владимир), в ООО «Электроприбор» (г. Москва), которые аналогичны по сетевой структуре СДО Палестины. Внедрение результатов исследований подтверждено соответствующими документами (см. приложения).

## Список литературных источников


1. Андреев А.А., Каплан С.Л., Краснова Г.А., Лобачев С.Л., Лупанов К.Ю., Поляков А.А., Скамницкий А.А., Солдаткин В.И.; Отв. ред. Солдаткин В.И. Основы открытого образования - Т. 1. - М.: НИИЦ РАО, 2002. - 676 с.
2. Галкин А.П. Информационная безопасность и целесообразные пути ее улучшения/ Palmarium Academic Publishing - Saarbrucken, Deuchland - 2014.75 с.
3. Андреев А.А. Введение в дистанционное обучение // Евразийская ассоциация дистанционного образования. Материалы IV Международной конференции по дистанционному образованию. - М.: МЭСИ, 1997.- 422 с.
4. Aljaradat M.M. The main tasks of designing a secure network-on-chip/Galkin A.P., Darahma I., Amro M.M.//Indian Science Cruiser. 2014, v. 28. N. 4. P.41-43.
5. Ефремов В.С. Виртуальное обучение как зеркало новой информационной технологии. // Менеджмент в России и за рубежом, 1999, № 6.-С.16-18.
6. 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.
7. 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
8. Васильев В.Н., Гугель Ю.В., Иванников А.Д., Ижванов Ю.Л., Тихонов А.Н., Хоружников С.Э. Состояние и перспективы развития телекоммуникационных технологий в сфере образования России // Телематика-2003: Труды X всерос. науч.-метод. конф. СПб., 2003. - с. 231-232.
9. Дунаев С. Доступ к базам данных и техника работы в сети. Практические

приемы современного программирования. М.: ДИАЛОГ- 1999.- 416 с.

10. Завьялова Н.Б. Методология разработки интегрированной информационной образовательной среды / Завьялова Н.Б., Дьяконова Л.П. // Информационные технологии в образовании: Сборник трудов участников XI конференции-выставки. Ч. IV. М.: МИФИ, 2001. - С. 133-134.
11. Бабешко В.Н., Нежурина М.И. О возможных подходах к оценке качества программных комплексов для образовательных сред // Электронные учебники и электронные библиотеки: Тез. докл. 3-й всерос. конф. — М.:МЭСИ, 2002.-с. 40-45.
12. Башмаков А.И., Башмаков И.А. Технология и инструментальные средства проектирования компьютерных тренажерно-обучающих комплексов для профессиональной подготовки и повышения квалификации // Информационные технологии . 1998, № 6, 7.
13. http://bugtraq.ru/library/internals/admintrap.html
14. Аль-Агбари Мохаммед. Защита телекоммуникаций систем дистанционного обучения Йемена от несанкционированного доступа к информации// Диссертация на соискание ученой степени кандидата технических наук/ Научный руководитель: Доктор технических наук, профессор Галкин А.П./ Владимирский государственный университет. г. Владимир-2008 – 170 с.
15. Зайцева Ж.Н., Рубин Ю.Б., Солдаткин В.И., Титарев Л.Г., Тихомиров В.П., Хорошилов А.В., Ярных В.В. Открытое образование: предпосылки, проблемы и тенденции развития / Под общей редакцией Тихомирова В.П. // Изд-во МЭСИ, М. 2000. - 178 с.
16. П.Белкин В.Ю., Костенко К.И., Левицкий Б.Е. Создание информационных ресурсов в электронной среде предметной области на основе типовых сценариев // Телематика-2003: Труды X всерос. науч.-метод. конф. СПб., 2003.-С.429-431.

17. Андреев А.Г. и др. Microsoft Windows 2000: Server и Professional. Русские версии / Под общ. ред. А.Н. Чекмарева и Д.Б. Вишнякова. - СПб.: БХВ-Петербург, 2002. - 1056 с: ил.
18. Дунаев С. Доступ к базам данных и техника работы в сети. Практические приемы современного программирования. М.: ДИАЛОГ- 1999.- 416 с.
19. 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
20. Карасик А.А. Доставка образовательного контента. Совмещение on-line и off-line режимов доступа к учебным ресурсам // Региональная многоуровневая система открытого образования Тверской области: Материалы третьей межрегион, науч.-практ. конф. Тверь, 2002 - С. 54-57.
21. Карасик А.А. Информационно-образовательная среда как способ интеграции учебных и организационных средств обеспечения дистанционного образования // Телематика-2002: Труды всерос. науч.-метод. конф. СПб., 2002.-С. 256-257.
22. Карасик А.А. Математическая модель электронного конспекта лекций как компонента электронного учебного курса // Телематика-2003: Труды X всерос. науч.-метод. конф. СПб., 2003. - С. 334-335.
23. Зайцева Ж.Н., Рубин Ю.Б., Титарев Л.Г., Тихомиров В.П., Хорошилов А.В., Усков В.Л., Филиппов В.М. Открытое образование - стратегия XXI века для России / Под общей редакцией Филиппова В.М. и Тихомирова В.П. // Изд-во МЭСИ, М. 2000.-324 с.
24. Зимакова М.В. Концепция построения интегрированной среды обучения. / Зимакова М.В., Зимаков В.Ф. // Университетское образование: Труды V МНТК. - Пенза, 2001 - часть П. - С. 47-52.
25. Игнатова И.Г. Образовательное пространство в системе ОРОКС // Телематика-2001: Труды междунар. науч.-метод. конф. СПб., 2001. -С. 89.

26. Карпенко М.П. Дистанционное образование в России: Проблемы теории и практики // Закон. Финансы. Налоги. - № 9(75) - 29 февраля - 2000.- С.34-38.
27. Карпов Е.Б., Фридланд А.Я., Фридланд И.А. Учебные материалы для открытого образования // Открытое образование. 2001, № 2. - С. 42-46.
28. Карасик А.А., Третьяков В.С. Электронные учебные курсы и их компоненты // Учебно-методическое обеспечение открытого инженерного образования: Материалы науч.-практ. семинара. Пенза, 2001. - С. 68-71.
29. Карасик А.А., Бурнев В.Б., Чубаркова Е.В., Третьяков В.С. Особенности технологии построения системы тестирования, как компонента обучающей среды // Современные технологии образования - фундамент будущего: Материалы докл. междунар. науч.-практ. конф. Минск, 2002. С. 40-43.
30. Карасик А.А., Третьяков В.С. Структура электронного учебника. Технология создания и использования // Технологии информационного общества — Интернет и современное общество: Труды V всерос. объединенной конф. СПб., 2002.-С. 189-191.
31. Корниенко В.В., Афанасьев А.Н. Модели и средства сетевого обучения XXXIV отчетная науч.-техн. конф. профессорско-преподавательского состава УлГТУ: тез. докл. Ульяновск, 2000.-214 с.
32. Кондратьев К.А., Белоногов А.Н. Техническое описание и концепция системы дистанционного обучения xDLS.- xDLSoft. http://www.xdlsoft.com/rus/doc/5_tech_ref.html (16 июня 2003).
33. Киселев Б.Г. Архитектура электронного учебника // Электронные учебники и электронные библиотеки в открытом образовании: Тезисы докл. 2-й всерос. конф. М.: МЭСИ, 2001. - С. 231-236.
34. Киреев А.Ю., Киреев Ю.В., Кравченко А.Н., Федин А.В. Открытому образованию открытые программы // Образование в информационную эпоху: Материалы междунар. конф. М., 2002. - С. 205-211.

35. Мамаев Е. Шкарина Л. Microsoft SQL Server для профессионалов. — СПб: Питер, 2001. - 1088 с.
36. Курганская Г.С. Модели, методы и технология дифференцированного обучения на базе Интернет: Автореф. дис. док. физ.-мат. наук. — М., 2001.-32 с.
37. Лобачев С.Л. Информационно - образовательная среда открытого образования: ход работы в 2001 году // Современная образовательная среда: Материалы всерос. конф. М.: ВВЦ «Наука и образование», 2001 - С. 110-115.
38. Лебедев В.Б. Кабакова И.В. Организация документооборота в системе дистанционного образования // Учебно-методическое обеспечение открытого инженерного образования: Материалы науч.-практ. семинара. Пенза, 2001. - С. 83-85.
39. Научное обеспечение открытого образования: Научно-методический и информационный сборник / Глав. ред. В.П. Тихомиров. М.: МЭСИ, 2000.-121 с.
40. Кривошеев А.О. Разработка и использование компьютерных обучающих программ // Информационные технологии. - 1996. - № 2. - С. 14-17.
41. Лобачев С.Л. Учебный процесс в системе открытого образования: опыт и перспективы. // Телематика-2003: Труды X всерос. науч.-метод. конф. СПб., 2003.-С. 443-449.
42. Обрайен Т., Подж С. Уайт Дж. Microsoft Access 97: разработка приложений: пер. с англ. - СПб.: БХВ - СПб., 1999. - 640 с.
43. Оболочка для создания распределенных обучающих и контролирующих систем (ОРОКС 2.1). Москва, МИЭТ, 1999.- 197 с.
44. Рогов С., Намиот Д. Тестирование производительности Web-серверов. Сибинфоцентр. http://www.sibinfo.ru/news/03_0 l_08/server_testing.shtm (17 июня 2003).
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. Российский портал открытого образования: обучение, опыт, организация/ Отв. ред. В.И. Солдаткин. - М.: МГИУ, 2003. - 508 с.

47. Соловов А.В. Информационные технологии обучения в профессиональном образовании // Информатика и образование . 1996, №1.- с. 13-19.

48. Солдаткин. В.И. Информационно-образовательная среда открытого образования // Телематика-2002: Труды всерос. науч.-метод. конф. СПБ., 2002. с. 281-284.

49. Титарев Д.Л. Сравнительный анализ современных САПР сетевых курсов // Открытое образование в России XXI века: Материалы Восьмой междунар. конф. М.: МЭСИ, 2000. - с. 228-231.

50. Технические и гуманитарные аспекты информационных образовательных сетей и сред: Монография /Под науч. ред. М.Ю. Монахова и И.В. Шалыгиной. - Владим. гос. ун-т, Владим. ин-т усоверш. учит., Владимир, 2001.-243 с.

51. Устинов В.А., Бусыгина Н.Г., Лозовная Н.Е., Кутенева И.В. Вопросы выбора системы управления учебным процессом для открытого образования //Телематика-2003: Труды X всерос. науч.-метод. конф. СПб., 2003. - с. 419-420.

52. Фролов А.В., Фролов Г.В. Базы данных в Интернете: практическое руководство по созданию Web-приложений с базами данных. — М.: Издательско-торговый дом «Русская редакция», 2000. - 432 с: ил.

53. Федорова Е.Ф. Системное представление дистанционного образования //Научно-методический журнал «Педагогические и информационные технологии в образовании». 2002, №5.

54. Христочевский С.А. Базовые элементы электронных учебников и мультимедийных энциклопедий // Системы и средства информатики: Вып.

9 / Под ред. И.А. Мизина. - М.: Наука. Физматлит, 1999. с. 202-214.

55. Ховард М., Леви М., Вэймир Р. Разработка защищенных Web-приложений на платформе Microsoft Windows 2000. Мастер-класс. / Пер. с англ. — СПб.: Питер; М.: Издательско-торговый дом «Русская Редакция», 2001. — 464 с: ил.
56. Aaron Skonnard. Understanding the IIS Architecture. 1999. http://www.microsoft.com/mind/1099/inside/insidel099.asp (26 апреля 2004)
57. Юрин В.Н. Компьютерные технологии в учебном процессе инженерного образования // Информационные технологии. 1999, №3.- с. 45-46.
58. Internet Information Server 4.0: Пер. с англ. - К.: Издательская группа BHV, 1998. - 624 с.
59. Hebenstreit J. Computers in education - The next step. // Education and Computing, v.l, 1995. -p. 37-43.
60. Siegfried Goschl, Microsoft Web Applications Stress Tool. JUGAT Meeting, 12 June 2001, www.javausergroup.at/events/was.pdf (17 июня 2003)
61. Open STA Documentation. Open System Testing Architecture Organization, www.opensta.org/docs/index.html (17 июня 2003).
62. Web Bench 4.1 Overview. TestingLabs, 2001, www.etestinglabs.com/benchmarks/webbench/home.asp (17 июня 2003)
63. А.С. № 855966 СССР, Генератор случайного импульсного потока, / Н.М.Ванина, А.П.Галкин и В.В.Орехов, опубл. 15.08.81. Бюл. №30
64. А.С. № 714638 СССР, Устройство для задержки импульсов, / А.П. Галкин, В.В.Аксенов и Ж.В.Аксенова, опубл. 05.02.80. Бюл.№5
65. А.С. № 842766 СССР, Генератор пуассоновского потока импульсов, / Н.М.Ванина, А.П.Галкин и В.В.Орехов, опубл.30.06.81. Бюл. №24.
66. WebStone 2.x Benchmark Description. Mindcraft, 1998, www.mindcraft.com/webstone/ws201-descr.html (17 июня 2003) XHTML 1.1 - Module-based XHTML. W3C Recommendation. 31 May 2001. http://www.w3.org/TR/2001/REC-xhtm111-2001(17 июня 2003)

67. Галкин А. П. Отношение дальностей при защите от несанкционированного доступа к информации./ Материалы 2-ой Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир, 1997, с.51-54
68. Галкин А. П. Оценка необходимости защиты информации предприятия. «Вестник ассоциации Русская оценка»,1999-1, с.55-58.
69. 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.
70. Галкин А. П. Целесообразность информационной защиты предприятия. / Материалы 3-ей Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир, 1999, с.64-67.
71. Ванина Н.М. Орехов В.В. Галкин А.П. Алгоритм управления качеством функционирования сложной системы связи, «Надежность и контроль качества», №3,1980, с.34-39.
72. Галкин А.П., Лапин А.Н., Самойлов А.Г. Моделирование каналов систем связи, М., Связь, 1979, 96 с.
73. Галкин А.П. Защита каналов связи предприятий и учреждений от несанкционированного доступа к информации./Уч. пос.- Владимирский государственный университет.- г. Владимир-2003. 126 с.
74. Галкин А.П. Радиосистемы для защиты каналов связи от несанкционированного доступа к информации./Уч. пос.- Владимирский государственный университет.- г. Владимир-2003. 104 с.
75. Саломаа А. Криптография с открытым ключом: Пер с англ.- М.: Мир, 1996.-318 с.
76. Петраков А.В. Основы практической защиты информации М.: Радио и связь, 1999.- 368 с.
77. Кочев А.Ю. и др. Предприниматель в опасности: способ защиты. М.: Юрфак МГУ, 1992,154 с Шлыков В.В. Безопасность предприятия в условиях рын-

ка: Учебное пособие для вузов.-Рязань: Горизонт, 1997.-148 с.

78. Петраков А.В. Защита и охрана личности, собственности, информации: Справ, пособие. -М.: Радио и связь, 1997. - 320с.

79. Горлов В.Н., Малафеев С.И. Применение многослойных нейронных сетей к решению задачи защиты информации./Проектирование и технология электронных средств, №2,2002

80. Защита программ и данных: Учебное пособие /П.Ю.Белкин, О.О.Михальский, А.С.Першаков и др.- М.: Радио и связь, 1999.-168с.

81. Петраков А. В. Основы практической защиты информации-М.: МТУСИ,2001. 310 с.

82. Datapro. Reports on Information Security, vol. 1-3, 1991-93, IS-001.

83. Петраков А. В. Основы практической защиты информации-М.: МТУСИ,2001. 310 с.

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

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

86. Калинцев Ю.К. Криптозащита сообщений в системах связи. Учебное пособие.-М.: МТУСИ, 2000.- 236 с.

87. Хорев А.А. Способы и средства защиты информации.- М.: МО РФ, 1999-316 с.

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

91. Галкин А.П., Аль-Агбари Мохаммед, Аль-Муриш Мохаммед, Суслова Е.Г. -Защита информации от несанкционированного доступа в системах обработки данных при физических экспериментах// Известия института инженерной физики. 2008-№3.-С.42-44.

92. Галкин А.П., Аль-Агбари Мохаммед, Аль-Муриш Мохаммед, Суслова Е.Г. -Защита информации от несанкционированного доступа в системах обработки данных при проектировании ЭС// Проектирование и технология электронных средств. 2007-№2.- С. 60-63.

93. Галкин А.П., Аль-Агбари Мохаммед, Идхилех Мохаммед, Падурянова Н.К. -Информационная защита прокси-серверов в проектировочных компьютерных сетях// Проектирование и технология электронных средств. 2007-№3.- С.

94. Галкин А. П., Аль-Агбари Мохаммед И. , Аркадьева М.С., Новикова С.В. – Целесообразность ставки на защищенные информационные системы. // Материалы 6-й Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир, 2007.- С.55-57.

95. Галкин А.П., Аль-Агбари Мохаммед, Идхилех Мохаммед, ПадуряноваН.К. Информационная защита прокси-серверов в компьютерных сетях // Материалы 8-й Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир, 2007.- С.52-54.

96. Галкин А.П., Аль-Агбари Мохаммед, А.К.М. Атаул Гани, Трещин П.С. Финансовая устойчивость и информационная безопасность/ «Экономика и управление: теория и практика». Матер. междунар. научн.
конф. Владимир, 2006.- С.39-44.

97. Галкин А.П., Аль-Агбари Мохаммед, А.К.М. Атаул Гани, Трещин П.С. Уменьшение рисков при информационных угрозах финансовым структурам/ «Экономика и управление: теория и практика». Матер. междунар. научн.конф. Владимир, 2006.- С.35-39.

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

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

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

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

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

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

104. Альджарадат М.М. Повышение отказоустойчивости транспортного уровня вычислительных сетей путем реорганизации сквозной «точка-точка» множественной адресации/ ГалкинА.П., Дарахма Ислам, 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. Альджарадат М.М. Обоснование аппаратурных затрат на реализацию итеративного кода для обнаружения и коррекции ошибок при информационной защите / Галкин А.П., Амро М.М, Дарахма Ислам // Проектирование и технология электронных средств №4, 2013. с. 20-23.

106. Альджарадат М.М. Минимизация при обеспечении информационной защиты в сетях / Галкин А.П., Бадван А., Дарахма Ислам, Яремченко С.В.// Известия института инженерной физики.2013. №1. С. 2-4.
107. http://www.mtit.pna.ps/ar/index.php
108. http://www.pma.ps/ar-eg/home.asp

**ПРИЛОЖЕНИЕ**

**Алгоритм и блок-схема программы.**

Выбор контролируемых параметров по максимальному значению вероятности безотказной работы после проведения диагностики.

Gy – ограничение на проведение контроля;

$g_k$ – затраты на контроль параметра;

$a_{ik}$ – двоичная матрица объектов контроля;

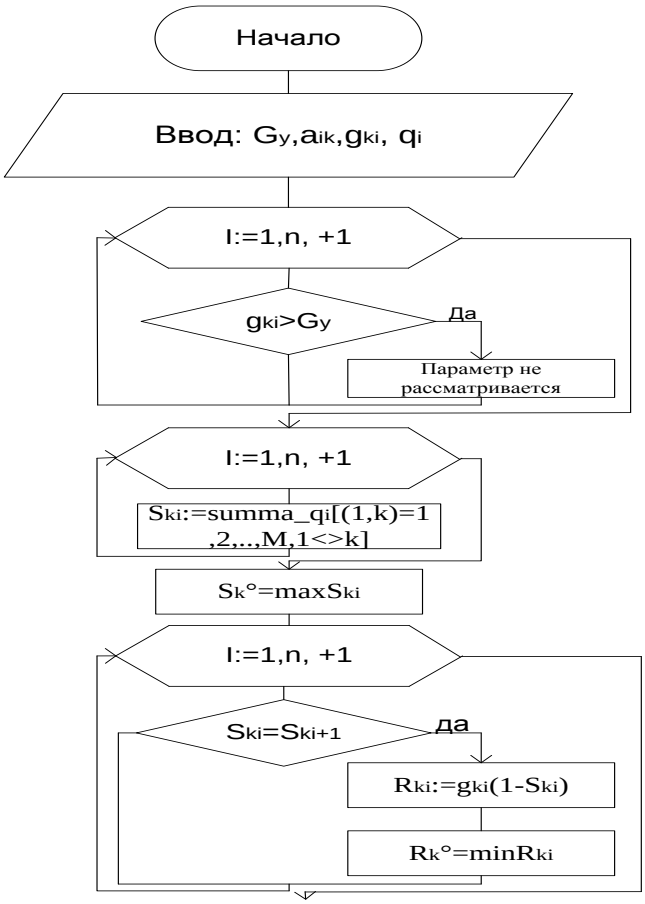
$q_i$ – априорные вероятности отказа i-того элемента;

$S_k$ – ненадежность k-го параметра ($\pi$k);

$P_{i(k)}$ – вероятность безотказной работы;

$\pi_k$– параметр;

$\pi^\circ_k$– оптимальный параметр;



Выбор контролируемых параметров по максимальным значениям.

$G_{1,2}$ – ограничение на выбор состава контролируемых параметров;

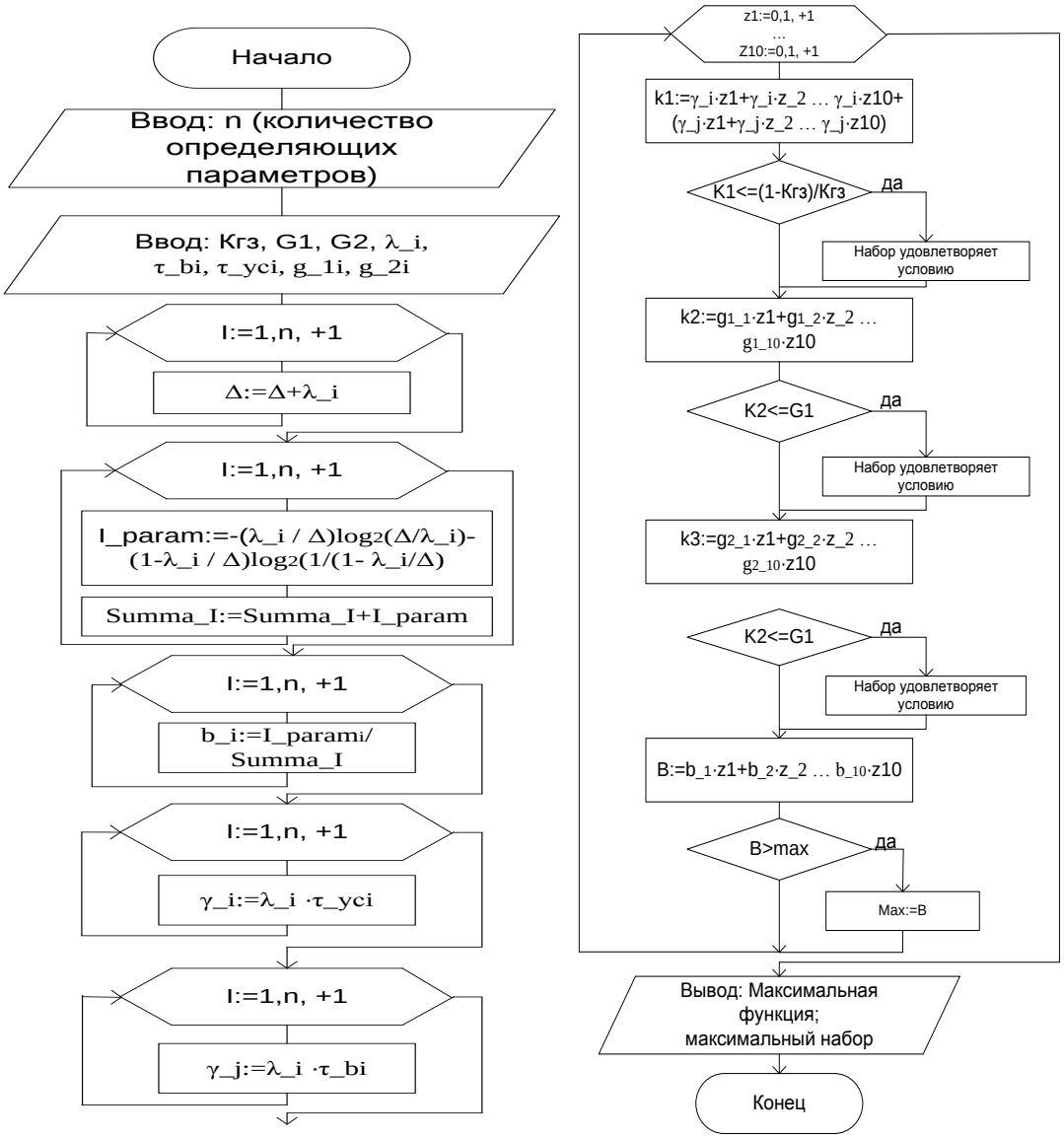
$g_{1,2}$ – достигнутое значение по s-му ограничению;

$\lambda_i$ – интенсивность проникновений в i-тый параметр;

$\Delta$– интенсивность проникновений в канал;

$\tau_{bi}$ – время восстановления i-го элемента;

$\tau_{yci}$ – время устранения неисправности i-го элемента;



Приложение 3.3.1.

41) I[i]=-0.0146741 I[40]=0.041 42) I[i]=-0.0149816 I[41]=0.042

43) I[i]=-0.0152879 I[42]=0.043 44) I[i]=-0.015593 I[43]=0.044

45) I[i]=-0.0158971 I[44]=0.045 46) I[i]=-0.0162 I[45]=0.046

47) I[i]=-0.0165018 I[46]=0.047 48) I[i]=-0.0168025 I[47]=0.048

49) I[i]=-0.0171023 I[48]=0.049 50) I[i]=-0.017401 I[49]=0.05

51) I[i]=-0.0176987 I[50]=0.051 52) I[i]=-0.0179954 I[51]=0.052

53) I[i]=-0.0182913 I[52]=0.053 54) I[i]=-0.018586 I[53]=0.054

55) I[i]=-0.01888 I[54]=0.055 56) I[i]=-0.019173 I[55]=0.056

57) I[i]=-0.019465 I[56]=0.057 58) I[i]=-0.0197563 I[57]=0.058

59) I[i]=-0.0200467 I[58]=0.059 60) I[i]=-0.0203363 I[59]=0.06

61) I[i]=-0.0206248 I[60]=0.061 62) I[i]=-0.0209127 I[61]=0.062

63) I[i]=-0.0211998 I[62]=0.0629999 64) I[i]=-0.0214861 I[63]=0.064

65) I[i]=-0.0217716 I[64]=0.065 66) I[i]=-0.0220563 I[65]=0.066

67) I[i]=-0.0223404 I[66]=0.067 68) I[i]=-0.0226236 I[67]=0.068

69) I[i]=-0.0229061 I[68]=0.069 70) I[i]=-0.0231879 I[69]=0.07

71) I[i]=-0.0234689 I[70]=0.071 72) I[i]=-0.0237493 I[71]=0.072

73) I[i]=-0.0240289 I[72]=0.073 74) I[i]=-0.024308 I[73]=0.074

75) I[i]=-0.0245862 I[74]=0.075 76) I[i]=-0.0248638 I[75]=0.076

77) I[i]=-0.0251409 I[76]=0.077 78) I[i]=-0.0254173 I[77]=0.078

79) I[i]=-0.0256929 I[78]=0.079 80) I[i]=-0.025968 I[79]=0.08

81) I[i]=-0.0262424 I[80]=0.081 82) I[i]=-0.0265162 I[81]=0.082

83) I[i]=-0.0267894 I[82]=0.083 84) I[i]=-0.0270621 I[83]=0.084

85) I[i]=-0.0273341 I[84]=0.085 86) I[i]=-0.0276055 I[85]=0.086

87) I[i]=-0.0278764 I[86]=0.087 88) I[i]=-0.0281466 I[87]=0.088

89) I[i]=-0.0284163 I[88]=0.089 90) I[i]=-0.0286855 I[89]=0.09

91) I[i]=-0.0289541 I[90]=0.091 92) I[i]=-0.0292221 I[91]=0.092

93) I[i]=-0.0294895 I[92]=0.093 94) I[i]=-0.0297566 I[93]=0.09

95) I[i]=-0.030023 I[94]=0.095 96) I[i]=-0.0302888 I[95]=0.096

97) I[i]=-0.0305543 I[96]=0.097 98) I[i]=-0.0308191 I[97]=0.098

99) I[i]=-0.0310835 I[98]=0.099 100) I[i]=-0.0313473 I[99]=0.1

101) I[i]=-0.0316107 I[100]=0.101 102) I[i]=-0.0318735 I[101]=0.102

103) I[i]=-0.0321359 I[102]=0.103 104) I[i]=-0.0323977 I[103]=0.104

105) I[i]=-0.0326591 I[104]=0.105 106) I[i]=-0.0329201 I[105]=0.106

107) I[i]=-0.0331806 I[106]=0.107 108) I[i]=-0.0334406 I[107]=0.108

109) I[i]=-0.0337 I[108]=0.109 110) I[i]=-0.033959 I[109]=0.11

111) I[i]=-0.0342176 I[110]=0.111 112) I[i]=-0.0344758 I[111]=0.112

113) I[i]=-0.0347335 I[112]=0.113 114) I[i]=-0.0349909 I[113]=0.114

115) I[i]=-0.0352477 I[114]=0.115 116) I[i]=-0.0355041 I[115]=0.116

117) I[i]=-0.03576 I[116]=0.117 118) I[i]=-0.0360155 I[117]=0.118

119) I[i]=-0.0362707 I[118]=0.119 120) I[i]=-0.0365253 I[119]=0.12

121) I[i]=-0.0367795 I[120]=0.121 122) I[i]=-0.0370335 I[121]=0.122

123) I[i]=-0.0372869 I[122]=0.123 124) I[i]=-0.0375399 I[123]=0.124

125) I[i]=-0.0377925 I[124]=0.125 126) I[i]=-0.0380448 I[125]=0.126

127) I[i]=-0.0382967 I[126]=0.127 128) I[i]=-0.038548 I[127]=0.128

129) I[i]=-0.0387991 I[128]=0.129 130) I[i]=-0.0390498 I[129]=0.13

131) I[i]=-0.0393001 I[130]=0.131 132) I[i]=-0.03955 I[131]=0.132

133) I[i]=-0.0397994 I[132]=0.133 134) I[i]=-0.0400486 I[133]=0.134

135) I[i]=-0.0402974 I[134]=0.135 136) I[i]=-0.0405457 I[135]=0.136

137) I[i]=-0.0407938 I[136]=0.137 138) I[i]=-0.0410415 I[137]=0.138

139) I[i]=-0.0412888 I[138]=0.139 140) I[i]=-0.0415357 I[139]=0.14

141) I[i]=-0.0417823 I[140]=0.141 142) I[i]=-0.0420285 I[141]=0.142

143) I[i]=-0.0422744 I[142]=0.143 144) I[i]=-0.0425199 I[143]=0.144

145) I[i]=-0.0427651 I[144]=0.145 146) I[i]=-0.0430099 I[145]=0.146

147) I[i]=-0.0432545 I[146]=0.147 148) I[i]=-0.0434985 I[147]=0.148

149) I[i]=-0.0437424 I[148]=0.149 150) I[i]=-0.0439858 I[149]=0.15

151) I[i]=-0.044229 I[150]=0.151 152) I[i]=-0.0444718 I[151]=0.152

153) I[i]=-0.0447142 I[152]=0.153 154) I[i]=-0.0449564 I[153]=0.154

155) I[i]=-0.0451982 l[154]=0.155 156) I[i]=-0.0454397 l[155]=0.156

157) I[i]=-0.0456809 l[156]=0.157 158) I[i]=-0.0459218 l[157]=0.158

159) I[i]=-0.0461623 l[158]=0.159 160) I[i]=-0.0464025 l[159]=0.16

161) I[i]=-0.0466424 l[160]=0.161 162) I[i]=-0.046882 l[161]=0.162

163) I[i]=-0.0471212 l[162]=0.163 164) I[i]=-0.0473602 l[163]=0.164

165) I[i]=-0.047599 l[164]=0.165 166) I[i]=-0.0478373 l[165]=0.166

167) I[i]=-0.0480753 l[166]=0.167 168) I[i]=-0.0483132 l[167]=0.168

169) I[i]=-0.0485506 l[168]=0.169 170) I[i]=-0.0487878 l[169]=0.17

171) I[i]=-0.0490246 l[170]=0.171 172) I[i]=-0.0492613 l[171]=0.172

173) I[i]=-0.0494975 l[172]=0.173 174) I[i]=-0.0497335 l[173]=0.174

175) I[i]=-0.0499693 l[174]=0.175 176) I[i]=-0.0502046 l[175]=0.176

177) I[i]=-0.0504398 l[176]=0.177 178) I[i]=-0.0506747 l[177]=0.178

179) I[i]=-0.0509093 l[178]=0.179 180) I[i]=-0.0511436 l[179]=0.18

181) I[i]=-0.0513776 l[180]=0.181 182) I[i]=-0.0516113 l[181]=0.182

183) I[i]=-0.0518448 l[182]=0.183 184) I[i]=-0.052078 l[183]=0.184

185) I[i]=-0.0523109 l[184]=0.185 186) I[i]=-0.0525435 l[185]=0.186

187) I[i]=-0.0527759 l[186]=0.187 188) I[i]=-0.0530079 l[187]=0.188

189) I[i]=-0.0532399 l[188]=0.189 190) I[i]=-0.0534714 l[189]=0.19

191) I[i]=-0.0537027 l[190]=0.191 192) I[i]=-0.0539338 l[191]=0.192

193) I[i]=-0.0541645 l[192]=0.193 194) I[i]=-0.0543951 l[193]=0.194

195) I[i]=-0.0546253 l[194]=0.195 196) I[i]=-0.0548554 l[195]=0.196

197) I[i]=-0.0550851 l[196]=0.197 198) I[i]=-0.0553146 l[197]=0.198

199) I[i]=-0.0555438 l[198]=0.199 200) I[i]=-0.0557729 l[199]=0.2

**«Утверждаю»**
**Генеральный директор**
**НПО «РИК»,** г. Владимир
**к. т. н.-**

11.11.14 **А. В. Поляков**

## Акт внедрения

Результаты, полученные **Альджарадат Махраном**(гражданин Палестины) при выполнении диссертационной работы, в частности:

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

2) Рекомендации по проектированию защищенных телекоммуникационных и компьютерных сетей с маршрутизаторами;

3) Использование минимизации маршрутизаторов для информационной защиты и анализ эффекта от этого; получен выигрыш на 70%;

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, уменьшают время проектирования в 2-3 раза и не требуют специальной подготовки нашего персонала.

Начальник отдела- Сирко С. Э.

Начальник лаборатории - Смушко О.Л.

**«Утверждаю»**

**Генеральный директор**

**ПФ «Электроприбор»** (г. Москва)

**Н. И. Захарова**

4 ноября 2014 г.

# Акт внедрения

Результаты, полученные **Альджарадат Махраном** (гражданином Палестины) при выполнении диссертационной работы, внедрены на нашем предприятии в 2013-14 гг. в виде расчетных методик и алгоритмов по проектированию защищенных сетей, в частности, с учетом экономической целесообразности защиты информации.

Особенно интересным для нас оказалось применение минимизации маршрутизаторов 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, что позволило уменьшить число маршрутизаторов в 2 раза, а время проектирования в 3 раза.

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

Администратор сети - **Володин А.И.**

بسم الله الرحمن الرحيم

University Graduates Union
Palestine Polytechnic University
(PPU)

رابطة الجامعيين / محافظة الخليل
جامعة بوليتكنك فلسطين

26.11.2014

**The certificate of introduction**

Results received from Mr. MAHRAN M.A. ALJARADAT at performance of Dissertation work are introduced at our University (Palestine Polytechnic University) enterprises in the form of settlement techniques and of economic feasibility of protection of the information. Check or presence of possible ways of penetration in communication systems of our University enterprise. Recommendation of safe computers and telecommunication networks from not authorized access of the information are used.

Dr. Ramzi Qawasma.
College of Engineering, Dean

College of Engineering,
Palestine Polytechnic University,
Hebron, Palestine.
P.O. Box 198.
e-mail: ramzi@ppu.edu
Phone: 00970-2-2233050
Mobile: 00970-599-078808

د. رمزي عبد الرحيم القواسمي
Dr. Ramzi A. Qawasma
+972 599078808

Совет выпускников Университета
**Палестинский политехнический университет**
**(ППУ)**

26.11.2014 г.

## Акт внедрения

Результаты, полученные г-ном Альджарадат Махран М.А. при выполнении диссертационной работы внедрены в нашем университете (Палестинском политехническом университете), в виде расчетных методик с учетом экономической целесообразности защиты информации. Проведена проверка на наличие возможных путей проникновения в системы связи нашего университета. Использованы рекомендации по защите компьютерных и телекоммуникационных систем от несанкционированного доступа к информации.

Г-н Рамзи Кавасма
декан инженерно-технического факультета *подпись.*

Инженерно-технического факультет
Палестинский политехнический университет
г. Хеврон, Палестина
а/я 198.
e-mail:ramzi@ppu.edu
Тел:00970-2-2233050
Моб. тел.: 00970-599-078808

Штамп: Г-н Рамзи Кавасма
+972 599078808



Перевод с английского языка на русский язык сделала переводчик Седунова Оксана Владимировна

***Город Владимир Владимирской области.***
***Двадцать восьмого ноября две тысячи четырнадцатого года.***

*Я, Зиновьев Валерий Анатольевич, нотариус нотариального округа города Владимир, свидетельствую подлинность подписи, сделанной переводчиком Седуновой Оксаной Владимировной в моем присутствии. Личность ее установлена.*

*Зарегистрировано в реестре за № **9п-11529.***

*Взыскано по тарифу:* *100 руб. 00 коп.*
*200 руб. 00 коп. взыскано за оказание услуг правового и технического характера.*

*Нотариус* *Зиновьев В.А.*

*Пронумеровано, прошнуровано и скреплено*

*печатью 2 (два) листа*

*Нотариус*