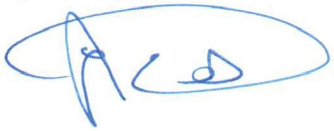
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

На правах рукописи



Обади Хезам Мохаммед Али

МЕТОДИКИ И АЛГОРИТМЫ ДЛЯ ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИОННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ ЙЕМЕНА

Специальность 05.12.13 – Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени
кандидата технических наук

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

Владимир-2015г.

СОДЕРЖАНИЕ

Список сокращений

АКС - Аппаратура конфиденциальной связи

АНБ - Агентство национальной безопасности (США)

АСУ - Автоматизированная система управления

АСУД - Автоматизированная система управления документооборотом

АШКУ - Абонентское шифрующее и кодирующее устройство

ГПСПИ - Генератор псевдослучайной последовательности импульсов

ЗАС - Аппаратура засекречивания

КИТС – компьютерная информационная телекоммуникационная система

КП - Коммутация пакетов

КПИ - Коэффициент потерь информации

КС - Канал связи

КТ – Конфиденциальная тайна

КЭВМ - Кодирующая электронно-вычислительная машина

НСД - Несанкционированный доступ

ОЗУ - Оперативное запоминающее устройство

ПК - Персональный компьютер

ПЭВМ - Персональная ЭВМ (ПК)

РЭС - Радиоэлектронные средства (радиоэлектронная система)

СОА – Система отражения атак

СОИ - Система обнаружения излучений

ТК - Технический канал

ТКУИ - Технический канал утечки информации

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

ТСР - Технические средства разведки

ТУ - Технические условия

ЦПОС - Цифровой процессор обработки сигналов

ШУ - Шифрующее устройство

УСКС - Устройство сопряжения с каналом связи

ЭЦП - Электронная цифровая подпись

UMTS - Универсальная мобильная телекоммуникационная система (Universal mobile telecommunications system)

Введение

В течение последних 5-10-ти лет в арабских странах мира наблюдается бурное развитие цифровых технологий, вызванное интенсивным внедрением компьютерных телекоммуникационных сетей и систем дистанционного образования (СДО) [1-14, 38-40]. Такой же подъем есть и в республике Йемен. Они усугубляются еще и становлением в ней информационных технологий и телекоммуникаций и пока с плохой информационной защитой [56,57, 91-97] табл.В.1:

Таблица В.1. Современные виды телекоммуникаций для СДО в арабских странах

особенности	Отношение к Йемену	трудности	Отношение к Йемену
неплотно заселенные территории	частично	недостаточный компьютерный парк учебных учреждений и индивидуальных пользователей (тьюторов и студентов)	полностью
невысокий жизненный уровень и неустойчивое политическое и экономическое положения	полностью	слабое развитие компьютерных телекоммуникационных сетей СДО, а иногда и устаревшее оборудование	полностью
Сосредоточение науки и образовательной элиты в нескольких крупных центрах	частично	недостаточная компьютерная грамотность и информационная культура населения	частично

большой уровень неудовлетворенного спроса на СДО и на телекоммуникационные услуги	полностью	Недоброжелательное окружение соседних стран	частично

Как видно, это относится к Йемену [41, 107].

Актуальность. На рынке арабских стран представлено достаточно большое число программных продуктов, но недостаточный компьютерный парк и устаревшее оборудование и недостаточная информационная культура населения создают трудности для осуществления информационного обеспечения процессов телекоммуникационного обмена. Однако большая их часть не удовлетворяет критериям, предъявляемым к ним с точки зрения защиты от несанкционированного доступа к информации[67], которая может быть эффективно реализована только в условиях качественных каналов связи. Это условие выполняется еще далеко не во всех даже центральных районах, не говоря уже о периферии в Йемене.

Одной из первых работ посвященной этой тематике для Йемена была диссертация Аль - Агбари Мохаммеда, 7 лет назад[8]. С тех пор изменилась технологическая база в стране, изменились ВУЗы. Данные проблемы рассматриваются уже с современных позиций. В то же время необходимо учитывать, что совместно с современным оборудованием некоторое время еще будет использоваться и устаревшее.

Понятно, что разработка информационно-программных сред, учитывающих требования современных образовательных учреждений Йемена и, в частности, защищенные СДО, а также особенности состояния сетевых коммуникаций в наших регионах, представляется чрезвычайно актуальным в современных условиях.

Особенно важно защищать образовательные учреждения для обеспечения их конкурентоспособности и для сохранения их функциональных

возможностей.

Объект исследования – системы корпоративных телекоммуникаций СДО и защита их от несанкционированного доступа к информации в условиях Йеменской недостаточности.

Цель работы- решение научно-технических задач, связанных с созданием комплекса методик и средств по обеспечению высокой информационной безопасности СДО Йемена и, следовательно, для повышения их конкурентоспособности. Для достижения указанной цели в диссертации сформулированы и решены следующие научные и технические задачи:

- анализ существующих программных продуктов, выполняющих функции защищенных информационных сред для СДО;
- оценка требований к структуре СДО и функциональным возможностям отдельных ее компонентов;
- рассмотрены и разработаны принципы и методики поиска технических устройств несанкционированного доступа к информации, которые могут быть реализованы при ограниченных возможностях СДО учебных заведений Йемена;
-разработана методика криптографической защиты от несанкционированного доступа;
- оценена эффективность информационного канала СДО с учетом защитных мероприятий;
- оценены показатели надежности, и уровень технического состояния защищаемого канала СДО;
- разработаны эффективные программы 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 и эксплуатации систем связи и передачи информации и в реальных СДО Йемена(см. внедрение в ТГУ, в приложении).

Научная новизна работы заключается в следующем:

- оценена целесообразность проведения защитных мероприятий для конкретных предприятий и учебных заведений для целей повышения их эффективности с учетом особенностей Йемена;

-на основе теорий надежности разработаны методики защиты информации в современной системе связи;

- впервые обоснован выбор криптографических средств защиты для СДО Йемена.

Практическая ценность работы. Разработанные методики и программные средства могут быть использованы в телекоммуникационных сетях конкретных образовательных учреждениях Йемена. При этом:

-проведены практические исследования предложенных схем защиты информации в корпоративной системе связи СДО Йемена, в том числе и с использованием криптографии;

-разработана структура и определены технические требования к современной многофункциональной системе связи СДО и защищенной передачи информации на основе использования разработанных методик;

-исследован выбор технических средств в защищенной системе связи СДО, что позволило предложить ряд методик, в том числе и с использованием криптографии; при этом число проникновений уменьшилось в 5 раз;

-в результате теоретических и экспериментальных исследований разработаны принципы поиска проникновений в канал, сохранение эффективности связи при этом;

-созданы методики определения целесообразности защиты информации в системах связи СДО Йемена;

-предложена методика повышения достоверности защищенных запоминающих устройств на 70%;

-программные продукты и методики по защите информации в каналах реализованы в образовательных учреждениях Йемена (ТГУ) и показали свою жизнеспособность и эффективность (см. приложения).

Основные положения, выносимые на защиту:

1. Оценка требований к структуре СДО и к функциональным возможностям отдельных ее компонентов.
2. Разработка принципов и методики поиска технических устройств несанкционированного доступа к информации, которые могут быть реализованы при ограниченных возможностях СДО учебных заведений Йемена.
3. Разработка методики криптографической защиты СДО от несанкционированного доступа.
4. Оценка эффективности информационного канала СДО с учетом защитных мероприятий и показатели надежности, и уровень технического состояния защищаемого канала СДО.
5. Разработка эффективных программ для поиска проникновений в телекоммуникации СДО.

Достоверность научных положений, выводов и практических результатов и рекомендаций подтверждена корректным обоснованием и анализом математических моделей рассматриваемых способов управления информационной безопасностью и защитой информации в СДО; наглядной технической интерпретацией моделей; данными экспериментальных исследований.

Результаты внедрения работы. Основные результаты внедрены в Таиз государственном университете (ТГУ), в Йемене, что подтверждено соответствующими документами.

Апробация работы. Основные научные и практические результаты работы докладывались и обсуждались на 4-х международных конференциях:

10-й международной научно технической конференции (НТК) «Перспективные технологии в средствах передачи информации», г. Владимир, 2013г.; 12-й международной научно-технической конференции «Физика и радиоэлектроника в медицине и экологии» (ФРЭМЭ), г. Владимир, 2012,2014гг.; Международной конференции НПК «Управление инновационными процессами развития региона», г. Владимир, 2012 г. межрегиональной научной конференции «Инновационное развитие экономики – основа устойчивого развития территориального комплекса», на 2-м международном экономическом конгрессе, г.Владимир- г.Суздаль- г. Москва,2013.

Публикации. Основное содержание работы изложено в 12-ти статьях и трудах НТК (из них 3 из списка ВАК), в отчетах Госбюджетных НИР кафедры радиотехники и радиосистем №118 (2012-2014гг.). На международных научно-технических конференциях и семинарах сделано 5 докладов и сообщений.

Структура и объем диссертации. Диссертация состоит из введения, 3-х глав, заключения, списка литературы, списка сокращений и приложений. Содержит 115 стр. основного текста, 108 библиографий, 45 табл., 31 рис.

Глава 1. Структура систем дистанционного обучения Йемена и необходимость защиты их телекоммуникаций от несанкционированного доступа

Дистанционное обучение - это получение образовательных услуг без посещения среднего или высшего учебного заведения с помощью современных информационных технологий и систем телекоммуникации, таких как электронная почта, телевидение и Интернет[21].

Система дистанционного обучения **(**СДО) это - комплекс организационных, учебно-методических, программных и аппаратных средств, обеспечивающий получение образования, в том числе и вне учебного заведения.

СДО понимается образовательная система на основе компьютерных телекоммуникаций с использованием современных педагогических и информационных технологий [14-20].

Дистанционное обучение можно использовать также для повышения квалификации и переподготовки учителей. Все это хорошо видно из табл.1.1.

Таблица 1.1. Основной состав СДО Йемена

состав	размещение	ответственность
администрация	ВУЗ, учебный центр	Правительство
технические специалисты	объединенные организационно	администрация
профессорско-преподавательский (тьюторы)	ВУЗ, учебный центр	Правительство, администрация
студенты	ВУЗ, учебный центр, территория страны	администрация
учебные материалы и продукты	Для одного или нескольких видов дистанционных технологий обучения	Администрация, тьюторы

методики обучения	Для одного или нескольких видов дистанционных технологий обучения	тьюторы
средства доставки знаний	объединенные организационно	Правительство, администрация

Проблема дистанционного обучения особенно актуальна для Йемена из-за неразвитости инфраструктуры, с огромной территорией и концентрацией научных центров и квалифицированных кадров только в крупных городах.

1.1. Классификация структур СДО

1.1.1. Наиболее используемые пути в СДО и их индикаторы

Количество информации, как и многие другие ее свойства не могут иметь место в качестве содержательных ориентиров СДО, они могут лишь служить некоторой ее мерой. Практика США, Европы и России показывает, на два типа содержательных ориентиров СДО. В обратном случае пришлось бы говорить о ценности информационных ресурсов СДО в зависимости от их общего количества, что не соответствует действительности.

1) *расширение доступности образования*. Это значит не только, расширение доступа для школьников и студентов, но и обеспечение непрерывного образования.

   Индикатор - увеличение числа учащихся.

2) *изменение качества образования:* усиление роли самостоятельного обучения, освоение новых информационных технологий, использование дополнительных образовательных ресурсов.

   Индикатор - расширение использования новых ресурсов в обучении.

1.1.2. Основы построения СДО

В качестве основы дистанционного обучения целесообразнее всего

использовать компьютерные телекоммуникации [22,23], которые предоставляют (табл.1.1.2.1):

Таблица 1.1.2.1. Возможности СДО

возможности	Предоставление
запрос информации по любому интересующему вопросу через электронные конференции	ВУЗы, пользователи
организация совместных телекоммуникационных проектов	Правительство, ВУЗы, пользователи
доступ к различным источникам информации	Правительство, ВУЗы
интерактивность и оперативная обратная связь	ВУЗы, пользователи
оперативная передача на любые расстояния информации любого объема и вида	Правительство, ВУЗы, пользователи

Формирующаяся сегодня в Йемене модель дистанционного обучения [24], в создании которой активное участие принимают ведущие ВУЗы, является, скорее, разновидностью заочного обучения, только с использованием компьютерных телекоммуникаций, но далеких от возможностей Европы, США и России. То, что это именно так хорошо видно из табл.1.1.2.2, 3.

Таблица 1.1.2.2. Основные экономические показатели в Йемене с 2000 г. по 2013 г. (млн. риалов)

Показатель	2000	2005	2010	2013
1. Полная потребительская корзина	114486	505363	1153526	2448559
2. Общие инвестиции	18406	112713	295011	595917
3. Баланс товаров и услуг	-7330	101433	112389	162500
4. Внутренний	125562	516643	1560926	3206976

валовой продукт по рыночной цене (1+2+3)				
Внутренний валовой продукт не нефтяных отраслей	108613	447527	1007385	2064395
5. Потребление постоянного капитала	5276	28845	92917	210683
6. Косвенные налоги	8295	27835	-28369	120057
7. Внутренний валовой продукт по цене производства (6-4)	117267	488808	1589295	3372919
8. Внутренний спрос (1+2)	132892	618076	1448537	3044476
9. Местные накопления (4-2)	11076	11280	407400	758417
10. Чистая прибыль от импортной продукции	-940	-22535	-114397	-295678
11. Национальный валовой продукт по рыночной цене (4+10)	124622	494108	1446529	2911298
12. Текущие переводы из за рубежа	16900	128774	215000	255689
13. Предоставленный национальный доход(11+12-5)	136246	594037	1568612	2956304
14. Накопления из предоставленных национальных доходов (13-1)	21760	88674	415086	507745
15. Накопления от национального валового продукта (11-2)	10136	-11255	293003	462739

Таблица 1.1.2.3.Внутренний валовой продукт (рыночные цены) и ВВП на душу населения с 2000 по 2013 гг. (текущие цены в млн. риалах)

Показатель		**2000**	**2005**	**2010**	**2013**
1. Численность населения в середине каждого года (в тысячах)		12860	15421	17162	20006
2. ВВП по рыночной стоимости		125562	515562	1560929	3206976
3. Чистая прибыль от переводов из-за рубежа		-940	-22535	-114397	-295678
4. ВВП не нефтяных отраслей		124622	494108	1446529	2911298
5. Средний курс доллара (в риалах)		13.92	100.00	161.73	191.42
6. ВВП по рыночной стоимости (U$)		8953	4941	8944	15209
7. Среднее на душу населения из ВВП	В риалах	9691	32041	84287	145521
	В долларах	696	320	521	760

1.1.3. Модели и особенности СДО

Существующие СДО можно разделить на несколько групп, в соответствии с предоставляемыми возможностями[1-9] (см. табл.1.1.3.1):

Таблица 1.1.3.1. Модели йеменских СДО

Особенности моделей	Обеспечение	действие
курсы дистанционного обучения	ВУЗ, тьютор	набор лекций, отправляемых пользователю порциями или целиком для самостоятельного изучения.
школьник, студент, абитуриент работает далее с ними дома, на рабочем месте, или в	студент	Тем самым учитываются индивидуальные способности и

специальном компьютерном классе		потребности пользователя
курсы дистанционного обучения снабжены терминологическими словарями	ВУЗ	содержат ссылки, открывающие доступ к отечественным и международным базам данных
периодическую отсылку по электронной почте выполненных пользователем заданий	тьютор, студент	рецензируются преподавателем-куратором и возвращаются к пользователю с замечаниями и рекомендациями
курсы дистанционного обучения включаются специальные компьютерные программы,	ВУЗ, тьютор, студент	могут проэкзаменовать пользователя, выявить ошибки, дать необходимые рекомендации, открыть доступ к электронным библиотекам

Создание последних упомянутых курсов обходится очень дорого. См. приложения.

1.2. Риски в телекоммуникациях СДО и критерии оценки защищенности от несанкционированного доступа

1.2.1. Природа рисков и необходимость инвестиций в информационную безопасность СДО Йемена

Инвестиции в информационную безопасность могут рассматриваться как инвестиции для увеличения прибыли путем уменьшения административных затрат на ее поддержание или для защиты от потери прибыли путем

предотвращения потенциальных затрат в случае негативных последствий [25-27] стоимость средств обеспечения безопасности должна соответствовать риску и прибыли для той среды, в которой используется данная СДО.

Как всегда и везде выделение финансовых и человеческих ресурсов на обеспечение безопасности ограничено, и требуется доказать прибыль от вложений в них (см. табл. 1.2.1.1):

Таблица 1.2.1.1. Риски, угрозы, уязвимости в СДО в Йемене

Риски, угрозы, уязвимости	Ответственность	обеспечение
риск - это ситуация, когда угроза использует уязвимое место для нанесения вреда вашей системе	Правительство, ВУЗы	Политика безопасности обеспечивает основу для внедрения средств обеспечения безопасности путем уменьшения числа уязвимых мест и как следствие уменьшает риск
анализ риска для оценки требуемой жесткости политики	Правительство, ВУЗы, администрация СДО	определит необходимые затраты на средства обеспечения безопасности для выполнения требований политики
Уровень угроз, которым подвергается СДО	ВУЗы, администрация СДО	видимость СДО из внешнего мира
Уязвимости СДО к последствиям потенциальных	администрация СДО	применение конкретных средств обеспечения

инцидентов с безопасностью		безопасности для конкретных объектов, модулей или приложений
Государственные законы и требования руководящих документов	Правительство, ВУЗы, администрация СДО	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

Следует отметить, что в данной работе как и в предложенных ранее работах не учитываются ценность информации или финансовые последствия инцидентов с безопасностью, тогда как зависимость государственных и коммерческих организаций от глобальных сетей становилась большей, потери от инцидентов с безопасностью, которые трудно оценить в деньгах, стали равными или большими, чем вычисляемые затраты. Это хорошо просматривается на сети в Йемене (рис.1.2.1.1)

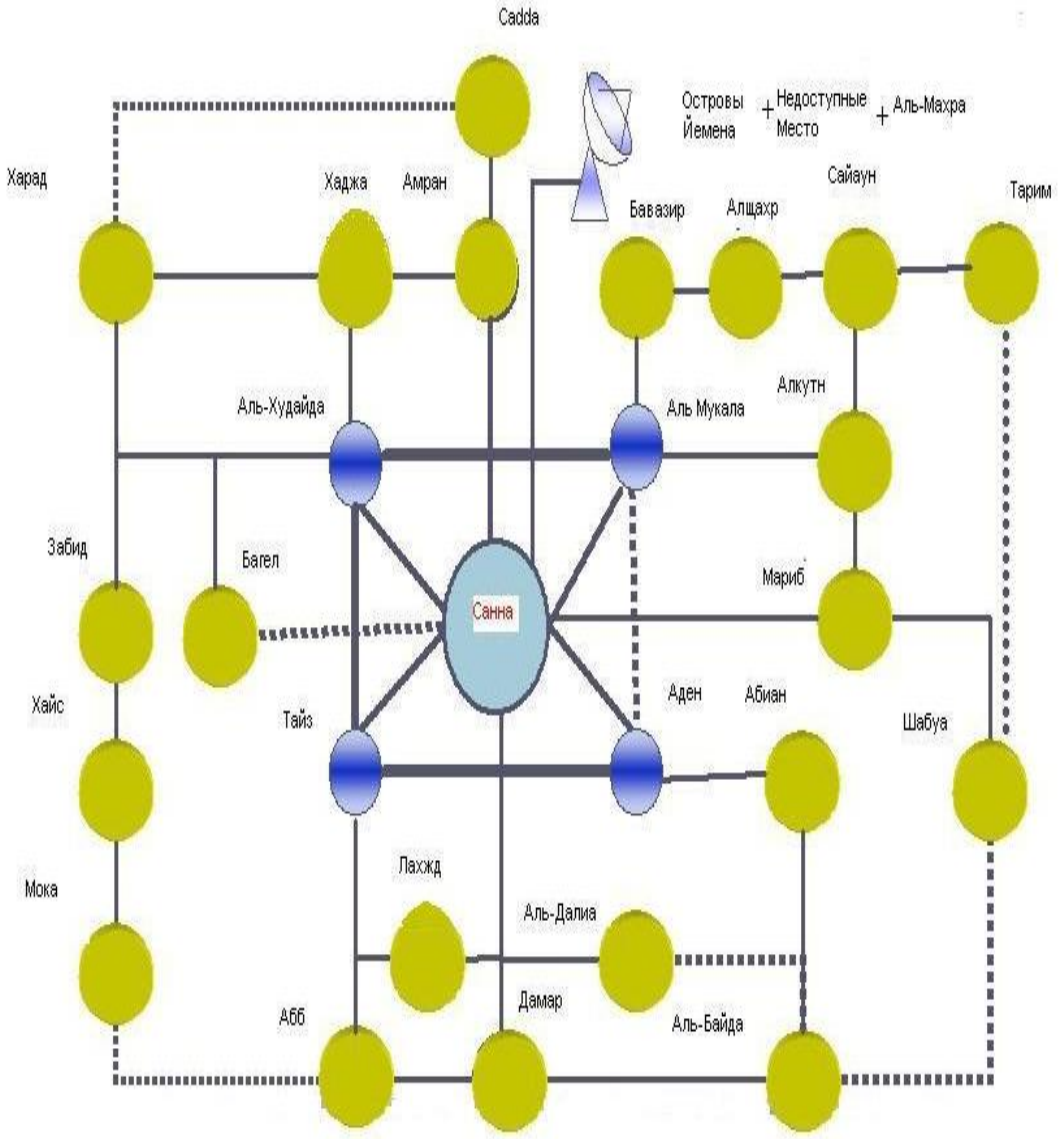


Рис. 1.2.1.1. Упрощенная структура сети СДО Йемена

Эти оценки стоимости требуются как составная часть формального анализа риска при затратах на безопасность [28-35].

Время администраторов может более эффективно потрачено на обеспечение конкретной, заданной, расчетной безопасности, чем на расчет стоимости *полной* безопасности.

1.2.2. Угрозы информационной безопасности в СДО

Умышленные угрозы могут быть разделены на ряд групп - от логичных (получение чего-либо без денег) до иррациональных (разрушение информации). Типичные сетевые и телекоммуникационные угрозы [36-40] (табл.1.2.2.1):

Таблица 1.2.2.1. Характерные угрозы СДО в Йемене

Угрозы умышленные	Источники	противодействие
Сканирование информации, неавторизованный просмотр критической информации злоумышленниками или авторизованными пользователями может происходить, используя различные механизмы - электронное письмо с неверным адресатом, распечатка принтера, неправильно сконфигурированные списки управления доступом, совместное использование несколькими людьми одного идентификатора и т.д.	хакеры, недобросовестные студенты, виновниками этого могут быть как внутренние, так и внешние пользователи	Паролизация, антивирусные программы, электронные подписи
Использование информации не по назначению - использование информации для целей, отличных от авторизованных, может привести к отказу в обслуживании, излишним затратам, потере репутации.	Конкуренты, хакеры, недобросовестные студенты, неквалифицированные тьюторы	электронные подписи
Сбой в работе одной из компонент телекоммуникационной сети из-за ошибок при проектировании или отказов оборудования или программ может привести к срыву в обслуживании или компрометации безопасности из-за неправильного функционирования одной из компонент	недобросовестные студенты, неквалифицированные тьюторы	антивирусные программы, поиск и устранение проникновений

телекоммуникационной сети		
Неавторизованное удаление, модификация или раскрытие информации- специальное искажение информационных ценностей, которое может привести к потере целостности или конфиденциальности информации	Конкуренты, хакеры, недобросовестные студенты	Паролизация, электронные подписи
замаскироваться под авторизованного пользователя для кражи сервисов или информации, или для инициации финансовых транзакций, которые приведут к финансовым потерям или проблемам для СДО	Конкуренты, хакеры, виновниками этого могут быть как внутренние, так и внешние пользователи	Паролизация, электронные подписи, поиск и устранение проникновений
Проникновение - атака неавторизованных людей или систем, несанкционированное изменение параметров телекоммуникационной сети которые могут привести к отказу в обслуживании или значительным затратам на восстановление после инцидента	Конкуренты, хакеры, недобросовестные студенты	электронные подписи, поиск и устранение проникновений

Видимость системы - это мера как интереса злоумышленников к этой системе, так и количества информации, доступной для общего пользования на этой системе. Поэтому, следует четко подразделять: угрозы, уязвимости, проникновения, риски.

Наличие угрозы необязательно означает, что она нанесет вред. Чтобы стать риском, угроза должна использовать уязвимое место в средствах

обеспечения безопасности системы и система должна быть видима из внешнего мира.

Так как многие угрозы, в Интернете, являются вероятностными (случайными) по своей природе, уровень видимости различных СДО напрямую определяет вероятность того, что враждебные агенты будут пытаться нанести вред с помощью той или иной угрозы [41-43].

Все СДО, имеющие доступ к Интернету, в некоторой степени видимы для внешнего мира хотя бы с помощью своего имени в DNS.

По мере того как использование глобальных сетей для электронной коммерции и критических задач увеличивается [44,45], число атак криминальных элементов и шпионов будет увеличиваться.

В Интернете любопытные и неопытные студенты, подростки-вандалы, криминальные элементы, промышленные шпионы могут являться носителями угрозы.

1.2.3. Пути и возможности информационной защиты СДО в Йемене

По сложившемуся мнению экспертов в политике защиты должны быть рассмотрены, по крайней мере, следующие аспекты [53] (табл. 1.2.3.1):

Таблица 1.2.3.1. Аспекты безопасности СДО в Йемене

НСД	Аспекты	Обеспечение
Хакеры, недобросовестные студенты, злоумышленники	безопасность телекоммуникационных сетей	Администрация, проект
Хакеры, злоумышленники	контроль прав доступа	Администрация
Хакеры, недобросовестные студенты, злоумышленники	мониторинг защиты и анализ статистики	Администрация, правительство

недобросовестные студенты	санкционирование доступа к компьютерным системам, идентификация и аутентификация пользователя	Администрация
злоумышленники	физическая безопасность	Администрация
Хакеры, злоумышленники	конфигурирование и тестирование систем	Администрация, правительство. проект
Хакеры, недобросовестные студенты, злоумышленники	обучение мерам безопасности	Администрация

Главная роль в безопасности СДО возлагается на процедуры идентификации и аутентификации [54,55]. Поэтому следует все-таки конфигурировать санкционирование доступа, не прибегая к установкам по умолчанию.

Стандартное средство для реализации этой функции - специальные файлы или списки хостов, с которых разрешен удаленный вход. Как показывают наши внедрения, этот тип защиты не в состоянии существенно уменьшить вероятность проникновения.

Снятие контроля имеет свои объяснения - обычно ссылаются на надежность других средств, отсутствие прямых входов, но предусмотреть все ситуации, возможные при работе с сетями, трудно.

Идентификация и аутентификация - это процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов.

Существуют такие виды аутентификации (табл.1.2.3.2):

Таблица 1.2.3.2. Аутентификация в СДО Йемена

Виды	обеспечение
Статическая аутентификация использует пароли и другие технологии, которые могут быть скомпрометированы с помощью повтора этой информации атакующим	пользователи
Устойчивая аутентификация использует криптографию [56-62] или другие способы для создания одноразовых паролей, которые используются при проведении сеансов работы.	Администрация, пользователи
Постоянная аутентификация предохраняет от вставки сообщений атакующим	Администрация

Активными атаками атакующий может активно воздействовать на соединение между пользователем и сервером.

Известны способы реализации борьбы с ними (табл.1.2.3.3)

Таблица 1.2.3.3. Атаки и борьба с ними в СДО Йемена

Отбой атак	Организаторы	воздействие
с помощью персонального устройства/документа, которым владеет только пользователь	Администрация, пользователи	смарт-карты, карманного аутентификатора или просто специально изготовленного удостоверения личности (предполагается, что аутентитификатор никогда никому не будет передаваться)
через аутентификацию самого пользователя	Администрация, проект, пользователи	по отпечаткам пальцев, голосу, рисунку сетчатки глаза и т.п. Эти методы

		опознавания развиваются в рамках биометрии
с помощью известного пользователю пароля или условной фразы	Пользователи	паролизация
комбинация этих способов	Администрация, проект, пользователи	Аутентитификатор, биометрия, паролизация

Современные программные технологии защиты способны снизить вероятность взлома системы, но не гарантируют высокой безопасности корпоративная телекоммуникационная сеть, в которой функционирует СДО включает реальный мир: пользователи, физические устройства, носители информации и т.д., которые также могут стать причиной неприятностей.

Все перечисленные аспекты информационной защиты так или иначе опираются на программные технологии, однако есть исключительно важные вопросы, выходящие из этого круга.

Наши пользователи (студенты, преподаватели старой формации), по-видимому в силу исторических традиций, относятся к вопросам секретности иронически.

Если взлом все же произошел, нужно быть готовым к тому, чтобы отреагировать очень быстро, пока злоумышленники не успели нанести тяжелых повреждений системе или заменить административные пароли.

1.2.5. Учет рисков и безопасности СДО

Для реализации стратегии защиты и можно и нужно самостоятельно убедиться, насколько наша система способна противостоять внешним атакам[47-53].

Для этого нужно найти ответы примерно на такие вопросы (табл.1.2.5.1):

Таблица 1.2.5.1. Конфиденциальность в СДО Йемена

Соответствие	Определение	признаки
Кто определяет	Администрация	что является конфиденциальным
Кто устанавливает состав конфиденциальной информации	Администрация, пользователи	сообщаемой персоналу для выполнения рабочих функций
Есть ли процедуры для работы	Администрация, проект	с конфиденциальной информацией
Кто администрирует систему безопасности	Администрация	на основе инженеров по безопасности

Самого пристального внимания заслуживает изучение материалов, опубликованных сотрудниками в Internet, в большинстве СДО таких документов нет или их игнорируют. Результаты изучения открытых материалов должны стать основой для внесения корректив в правила подготовки открытых изданий и тьюторов. Злоумышленник может извлечь изрядную долю фактически приватной внутренней информации СДО, покопавшись в ее открытых, публично доступных материалах.

Тогда придется проводить наблюдения за рабочими местами, определяя заодно, можно ли вообще заметить проявления какой-либо единой политики.

1.2.6.Анализ безопасности серверов СДО

В отличие от хост-систем серверы файлов, приложений, баз данных более молоды и сравнительно менее оттестированы - для многих из них возраст аппарата защиты насчитывает всего несколько лет. Большая часть таких

средств претерпевает постоянные и иногда очень существенные обновления. Часто, к сожалению, и администрирование серверов ведется специалистами с небольшим опытом, так что безопасность этого класса систем обычно оставляет желать много лучшего. Ситуация усугубляется тем, что, по определению, к серверам имеют доступ совершенно разнообразная публика по телефонным или другим линиям связи. Следовательно, оценка безопасности серверов требует повышенного внимания.

Для этого существует некоторое количество средств.

Продукты такого рода обследуют серверы (используя привилегированный доступ) и составляют отчет о конфигурации, практике администрирования системы защиты и популяции пользователей. Использовать автоматические средства имеет смысл - однократное сканирование может выявить проблемы, которые вряд ли можно обнаружить даже многими часами ручного анализа. Например, сканирование может быстро выявить процент пользователей, которые имеют излишне высокий уровень прав доступа или являются членами слишком многих групп.

Чтобы представить фронт работ покажем упрощенную структуру Тайз университета в Йемене (ТГУ) рис.1.2.6.1.

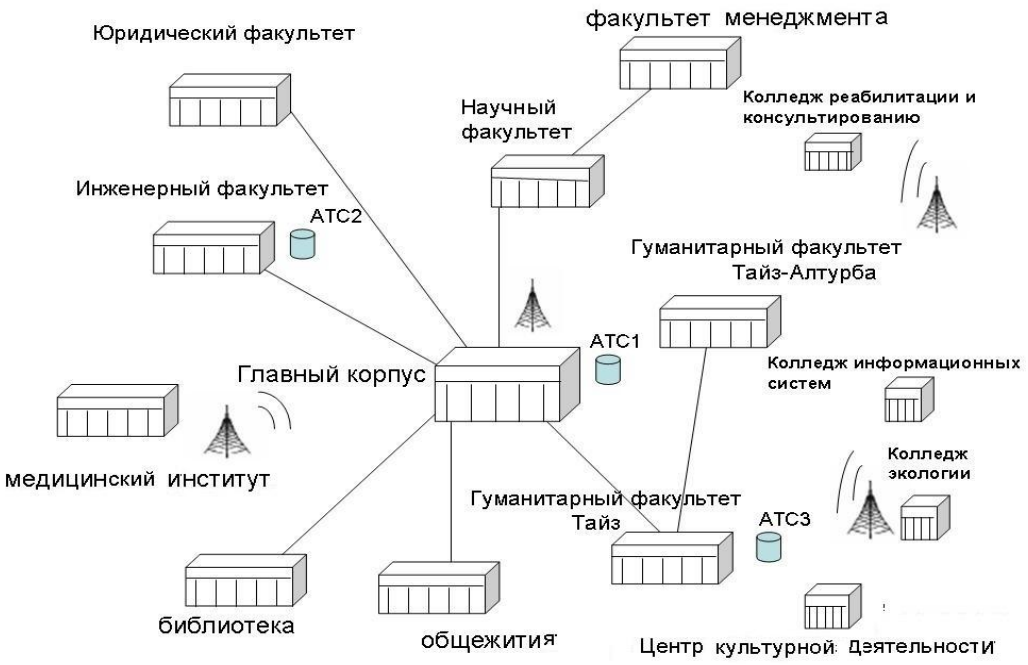


Рис.1.2.6.1.Упрощенная структура Тайз университета в Йемене (ТГУ)

1.2.7. Возможности защитных мероприятий СДО Йемена

Основой СДО является высококачественная и высокотехнологичная информационно-образовательная среда. Ее создание и развитие представляет технически сложную и дорогостоящую задачу, но она позволит системе образования коренным образом модернизировать свой технологический базис, перейти к образовательной информационной технологии в широком смысле этого слова и осуществить прорыв к открытой образовательной системе, отвечающей требованиям постиндустриального общества.

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.1.2.7.1):

Таблица 1.2.7.1. Мониторинг информационных потоков в СДО Йемена

Процессы	Обеспечение
обеспечение условий государственного регулирования информационных взаимодействий на основе лицензионной системы	Правительство, администрация
анализ процессов движения (потребления) информационных ресурсов в СДО и разработку рекомендаций по повышению эффективности их использования	администрация, проект
классификацию информационных массивов по максимально возможному числу параметров	администрация, пользователи, проект
перепись, регистрацию и учет основных информационных массивов	Правительство, администрация, проект

Необходимо предусмотреть создание в рамках СДО Йемена организационно-правовых механизмов (табл. 1.2.7.2):

Таблица 1.2.7.2. Организационные механизмы СДО Йемена

механизмы	Ответственность	действие
юридическая ответственность за неправомочные действия	Администрация	реализации различных видов ответственности за неправомочные действия
порядок оформления допуска	Администрация, тьюторы	допуск и доступ к указанным сведениям
порядок обмена сведениями	Администрация, проект, тьюторы	обмен этими сведениями при различных нормах отображения информации на материальных носителях
критерии перечней	Администрация	формирование сведений конфиденциального характера, порядок и сроки их пересмотра
организация работы	Администрация, проект	состав и правомочия тьюторов
порядок сведений к категориям	Администрация	отнесения сведений к категории ограниченного доступа

Перед подсистемой защиты информации [70] должны быть поставлены следующие конкретные задачи (табл.1.2.7.3):

Таблица 1.2.7.3. Задачи защиты в СДО Йемена

Задачи	Обеспечение	действие
разграничение прав доступа авторизованных пользователей системы к ее	Администрация. проект	основано на разделении субъектов и объектов по полномочиям, группам,

ресурсам,		категориям и тематикам
авторизация	Администрация. Тьюторы	преподавателей и обучающихся в процессе их взаимодействия
авторизация персонала	Администрация. Проект	Тех, кто управляет функционированием системы
защита ресурсов СДО	Администрация. Тьюторы	системы дистанционного обучения от несанкционированной установки, копирования и использования, обеспечение их целостности и подлинности

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

Целесообразно предусмотреть проведение исследований и работ по следующим направлениям (табл.1.2.7.4):

Таблица 1.2.7.4. Направления СДО Йемена

Направления	Ответственность	обеспечение
Разработка методов, методик и средств	Администрация, проект	обеспечение информационной безопасности корпоративной сети (первая и одна из основных наших задач)
Создание систем мониторинга и аудита	Администрация, проект, пользователи	информационной безопасности и сертификации программных и аппаратных средств информационной среды СДО (вторая и одна из основных

		наших задач)
Создание организационно-правовых и программных механизмов	Администрация, проект	управление информационными ресурсами с ограниченным доступом в СДО, обеспечивает защиту интересов правообладателей и пользователей
Разработка методов, методик и средств защиты ресурсов СДО	Администрация, проект, пользователи	от несанкционированной установки, копирования, модификации и использования, обеспечения их целостности и подлинности
Разработка технических и организационно-правовых методов	Администрация, пользователи	защита используемых в СДО методических и теоретических разработок, информационных ресурсов, авторских курсов, учебников, учебных пособий в целях сохранения коммерческой тайны, соблюдения авторских прав и прав на интеллектуальную собственность

Основными результатами работы в СДО Йемена должны стать (табл.1.2.7.5):

Таблица 1.2.7.5. Результаты улучшения в СДО Йемена

Результаты	Обеспечение	Что дает
Повышение эффективности проектирования сетей СДО	Правительство, администрация, проект	отвечает современным требованиям уровня подготовки в области информационных технологий

		(одна из основных наших задач, которая должна быть достигнута)
Создание единой системы	Правительство, администрация	обеспечивает информационную и научно-методическую поддержку образовательного процесса, оказание консультационных услуг
Предоставление условий для полноценного образования	Администрация	необходимость специального обучения различным группам населения
Развитие персонализации процесса обучения	Правительство, администрация	на основе организации индивидуальных образовательных траекторий
доступ к информационным ресурсам СДО	администрация	Корректный и тактичный доступ учащихся и преподавателей из других учебных заведений
Повышение качества обучения в СДО	Правительство, администрация, проект	Создание и применение методик оценок

1.3. Информационная безопасность и финансовые проблемы в республике Йемен при создании СДО

В подтверждение стратегической направленности инвесторам предоставляются различные выгоды, которые создают привлекательную деловую инвестиционную среду.

Информационная безопасность и финансовые проблемы являются особенностью двадцать первого века, и, практически не существует таких

государств, которые не сталкивались бы с ними. Большое количество таких проблем не миновало и Йемен.

Йемен обладает двусторонними соглашениями и протоколами сотрудничества с более чем 20 странами, и является членом Агентства многосторонних инвестиционных гарантий (MIGA).

После того, как перестала существовать монополия на стационарную телефонную линии в конце 2004 у иностранных инвесторов появились многочисленные возможности.

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

1.3.1. Природа коммерческих учебных заведений (акционерных обществ) и принципы их организации. Необходимость информационной защиты

Акционерное общество как система не может функционировать вне взаимосвязей с внешней средой, оказывающей на условия и результаты его деятельности существенное влияние, и поэтому является открытой системой, находящейся в непрерывном взаимодействии с другими, иными словами, само является под системой более общей экономической системы высшего уровня. А все это невозможно без систем телекоммуникаций и их информационной защиты.

1.3.2. Защита информации в беспроводных сетях коммерческих организаций

Решением подобных проблем нужно заниматься комплексно. Если политика безопасности беспроводной сети построена на MAC-адресах, то сетевая карта или точка доступа, украденная злоумышленником, может открыть доступ к вашей сети. Защиту информации при подключении к сети таких устройств сотрудники обеспечивают самостоятельно, не всегда задумываясь о последствиях. Что касается мероприятий технического

характера, то весьма хорошей результат достигается при использовании обязательной взаимной аутентификации устройств и внедрении активных (Obrserver 8.3, Airopeek NX 2.01, WirelessSniffer 4.75) и пассивных (APTools 0.1.0, xprobe 0.0.2) средств контроля.

1.3.3. Современные требования к защите СДО Йемена

Рекомендуется распределять пользователей с разной степенью защищенности по разным виртуальным ЛС и в соответствии с этим реализовывать свою политику безопасности.

Таблица 1.3.3.1

Критерий	**Подход**			
	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

Выводы по главе 1

1. Показана актуальность систем дистанционного обучения для Йемена.
2. Рассмотрены основные проблемы в СДО в Йемене и известные пути их решения и намеченные нами пути.
3. Обоснована необходимость защиты телекоммуникаций СДО от несанкционированного доступа к информации с учетом особенностей Йемена, так как рассмотренные методики и структуры не обеспечивают необходимое качество и защищенность сетей.

Глава 2. Методики оценок эффективности СДО в Йемене

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

При диагностике канала СДО 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)[55]. Под ПИП понимается число дополнительных связей при защите канала. Причиной их появления чаще всего являются или недостаточная квалификация обслуживающего персонала, или недостаточная защита. Необходимо оценить 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

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

Поэтому при автоматических мероприятиях по защите канала (АМЗК) СДО время использования за счет ПИП находится из соотношения [54,55]

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

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

В предположении того, что при отказах элементов любых типов величина $P_{\text{п}}$ = const, при АМЗК используем готовое выражение, полученное Галкиным А.П.[54,55]

$$\text{К}_{\text{пнАМЗК}} = 1 + \frac{P_{\text{АМЗК}} P_{\text{пу}} + (1 - P_{\text{АМЗК}}) P_{\text{п}}}{1 - P_{\text{АМЗК}} P_{\text{пу}} - (1 - P_{\text{АМЗК}})\, P_{\text{п}}}\ ,$$

где $P_{\text{АМЗК}}$ – вероятность того, что отказ вызван элементом, контролируемым АМЗК:

$$P_{\text{АМЗК}} = \frac{\sum_{i \in W} \lambda_i}{\Lambda}.$$

Данная методика была применена для расчетов при внедрении защитных мероприятий в ТГУ (см. приложения), разработав алгоритм и программу для этих расчетов. Расчеты для ТГУ.

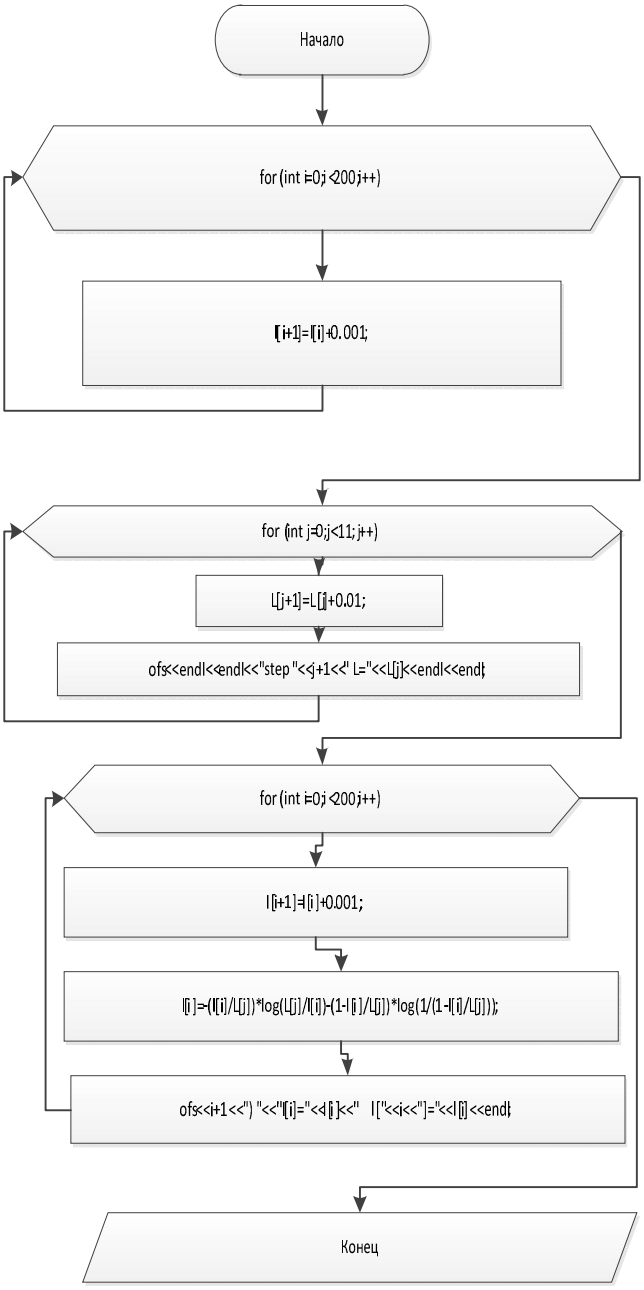


Таблица 2.1.1. Показатели КК кафедры химии ТГУ

наборы	**$P_{по}$**	**$P_{пу}$**	**$P_{амзк}$**	**$K_{амзк}$**
1	**0, 2**	**0, 6**	**0, 8**	**0,6**
2	**0, 5**	**0, 1**	**0, 5**	**0,5**
3	**0, 1**	**0, 2**	**0, 4**	**0,9**

Таблица 2.1.2. Показатели КК кафедры биологии ТГУ

наборы	**$P_{по}$**	**$P_{пу}$**	**$P_{амзк}$**	**$K_{амзк}$**
1	**0, 1**	**0, 5**	**0, 7**	**0,5**
2	**0, 3**	**0, 2**	**0, 5**	**0,5**
3	**0, 1**	**0, 2**	**0, 4**	**0,3**

Таблица 2.1.3. Показатели КК кафедры психологии ТГУ

наборы	**$P_{по}$**	**$P_{пу}$**	**$P_{амзк}$**	**$K_{амзк}$**
1	**0, 2**	**0, 4**	**0, 3**	**0,6**
2	**0, 1**	**0, 3**	**0, 2**	**0,7**
3	**0, 1**	**0, 2**	**0, 1**	**0,3**

Таблица 2.1.4. Показатели КК кафедры информатики и защиты информации ТГУ

наборы	**$P_{по}$**	**$P_{пу}$**	**$P_{амзк}$**	**$K_{амзк}$**
1	**0, 3**	**0, 3**	**0, 2**	**0,9**
2	**0, 2**	**0, 1**	**0, 5**	**0,5**
3	**0, 1**	**0, 2**	**0, 5**	**0,8**

Примечание: набор 1- повышенная достоверность ЗУ(2.2); 2- шифрование с нашими методиками и алгоритмами(2.3); 3=1+2.

2.2. Достоверность запоминающих устройств сетей СДО Йемена

Оценку достоверности функционирования отказоустойчивых запоминающих устройств (ЗУ) рассмотрим на примере ТГУ с

использованием кодирования (шифрования).

Отправитель знает ключ шифрования и принимающая сторона знает ключ для расшифровки.

Предлагаем разработанный нами алгоритм, реализующий возможности ЗУ с ограниченным объемом.

Алгоритм

Выберите больших простых чисел p и q такие, что p ~ = q.

Вычислить N = P*q

Вычислить φ (pq) = (p-1) * (q -1)

Выберите такой режим, что

gsd (φ (n), e) = 1; 1 <e <φ (n)

Выберите секретный ключ d такой, что

d * e mod φ (n) = 1

Таким образом, в RSA алгоритм шифрования и дешифрования являются осуществляется AS-шифрование рассчитать шифрованный текст C с открытым текстом M такой, что

C = M ^ e mod n

Расшифровка

M = C ^ d mod n = M ^ ed mod N

Сравнительный анализ алгоритмов

Были изучены различные методы, используемые для выполнения целей шифрования данных. Есть некоторые сравнения, полученные на разных важных функциях, такие как:

Ввод данных. Пространство памяти, необходимое M.

Построения M, определяется на основе размера входных данных, числа разрядов и т.д. Алгоритм считается лучшим тот, при котором используются мало оперативной памяти память.

Предел- времени, необходимого на алгоритме, чтобы завершить операцию зависит от скорости процессора, сложности алгоритма. **Пропускная способность**- рассчитывается путем деления общего открытого текста в

мегабайтах в зашифрованном виде на общее время шифрования для каждого алгоритма.

Теоретический анализ Теоретический анализ состоит в следующем группировании, приведенном в табл.2.2.1:

Таблица 2.2.1. Группирование ключей и алгоритмов

Характеристики	DES	Тройной DES	RSA
Используемый ключ	Один и тот же ключ используется для шифрования и дешифрования	Один и тот же ключ используется для шифрования и дешифрования	Разные ключи используются для шифрования и Расшифровка цель
Масштабируемость	Это масштабируемый алгоритм всилу изменения размера ключа и блока	Это масштабируемый алгоритм всилу изменения размера ключа и блока	Не масштабируемый алгоритм
лавинный эффект	не подвергается воздействию	не подвергается воздействию	подвергается воздействию
Потребляемая мощность	Низкая	Более чем DES и менее чем RSA	Высокая
пропускная способность	Очень высокая	высокая	Низкая
Конфиденциальность	высокая	Очень высокая	Низкая

Для моделирования использовались Java и ASP.NET были взяты два параметра времени и памяти для установки моделирования и расчёта пропускной способности путем деления общего открытого текста на шифрованное для каждого алгоритма.

Таблица 2.2.2. Время выполнения шифровки (миллисекунды)

Входной размер (кб)	3 DES	DES	RSA
45	50	25	55
55	44	29	46
96	76	45	89
236	113	79	119
319	155	89	157
560	177	131	179
899	299	240	369
5345.28	1166	1296	1441
Пропускная способность (мб/с.)	2.08	3.01	1.67

Таблица 2.2.3. Время выполнения (миллисекунды) расшифровки

Входной размер (кб)	3 DES	DES	RSA
45	45	36	55
55	42	31	48
96	65	49	73
236	104	88	105
319	135	89	157
560	160	131	169
899	181	152	173
5345.28	845	785	880
Пропускная способность(мб/с.)	4.03	5.012	2.147

Такая малая разрядность характерна для Йемена.

В этом случае[104]:

$$\lambda_i = 1*10^{-9}\ 1/ч, (\ p(t) = e^{-10^{-9}*t}). \qquad (2.2.1)$$

Вероятность безотказной работы накопителя по одному выходу равна[104]:

$$p1(t) = p(t)^{6M}. \qquad (2.2.2)$$

Достоверность функционирования отказоустойчивого ЗУ оценим используя выражение [104]:

$$D(t) = p_{ДЕК}(t)\sum_{i=0}^{k-1} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i + p_{ДЕК}(t)\sum_{i=1}^{n} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i - \quad (2.2.3)$$
$$P_{ДЕК}(t)^2 \sum_{i=0}^{k-1} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i * \sum_{i=1}^{n} C_n^i p1(t)^{(n-i)}[1-p1(t)].$$

Проведем оценку влияния кратности исправляемой ошибки аппаратурные затраты и достоверность функционирования устройств памяти при реализации кодирования информации при различных кратностях ошибок[104] (см. табл. 2.2.4-7).

Полученные результаты и зависимости, отображающие достоверности функционирования запоминающего устройства от времени, приведены в табл.2.2.4-7.

Таблица 2.2.4 – Набор ошибок от 0 до 3 (корректируется 88%)

Контролируемый параметр	**Всего**	**Корректируемых**	**0ош.**	**1ош.**	**2ош.**	**3ош.**
Общее количество ошибок	11111	9870	16	256	1800	9200
Некорректируемые	16	-	-	-	-	-
Имеющие совпадения	1300	-	-	0	0	1300
Без совпадений	9900		-	256(16)	180(110)	7900(491)
Только в информационных	224	224(14)	-	64	96	64
Только в контрольных	4800	4500(276)	-	200	960	3300
И в контрольных и в информационных	6144	5224(328)	-	0	704	4520

Таблица 2.2.5 - Набор ошибок от 0 до 4 (корректируется 59%)

Контролируемый параметр	**Всего**	**Корректируемых**	**0ош.**	**1 ош.**	**2 ош.**	**3 ош.**	**4 ош.**
Общее количество ошибок	40300	23700	16	256	1900	8960	29000
Некорректируемые	16	-	16	-	-	-	
Имеющие совпадения	16600	-	-	80	848	3104	12576
Без совпадений	23600		-	176(11)	1072(67)	5800(366)	16500(1034)
Только в информационных	240	144(9)	-	48	48	48	0
Только в контрольных	12688	9232(577)	-	128	704	2496	5904
И в контрольных и в информационных	27328	14272(892)	-	0	320	3312	10640

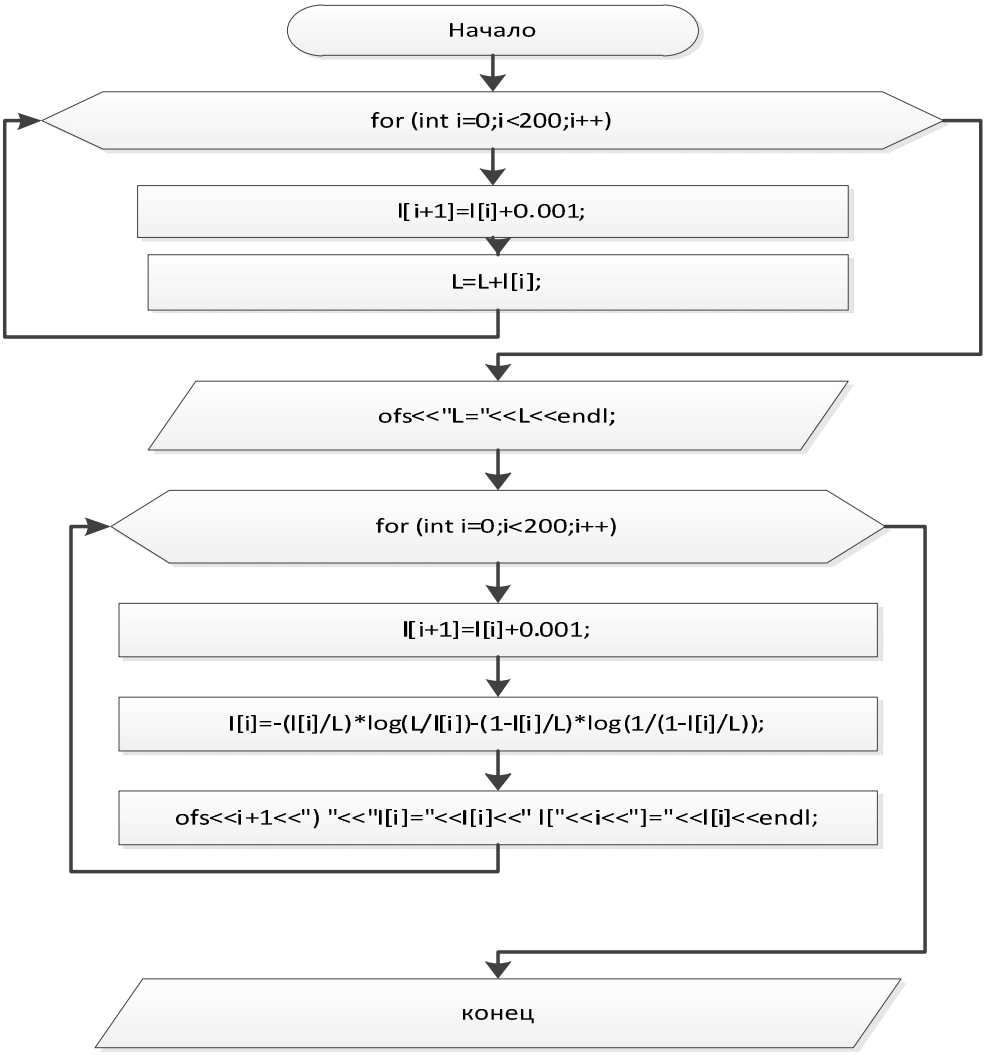
Таблица 2.2.6 – Набор ошибок от 0 до5 (корректируется 17%)

Контролируемый параметр	**Всего**	**Корректируемых**	**0 ош**	**1ош.**	**2 ош.**	**3 ош.**	**4 ош.**	**5 ош.**
Общее количество ошибок	110160	18944	16	256	1920	8960	29120	69888
Некорректируемые	32	-	16	-	-	-		16
Имеющие совпадения	91216	-	-	256	1520	7680	23200	58560
Без совпадений	18944		-	0	400(25)	1280(80)	5920(370)	11312(707)
Только в информационных	240	16(1)	-	0	16	0	0	0
Только в контрольных	25360	7552(472)	-	0	256	768	2176	4352
И в контрольных и в информационных	84528	11376(711)	-	0	128	512	3744	6960

Таблица 2.2.7-Числовые значения множеств групп n, l для ошибок кратности 0-5

Множество групп	**Кратность ошибки**		
	0-3	**0-4**	**0-5**
n_1	16	11	0
n_2	110	67	25
n_3	491	366	80
n_4	-	1034	370
	0-3	**0-4**	**0-5**
n_5	-	-	707
l_1	14	9	1
l_2	276	577	472
l_3	328	892	711

Используя данные из таблиц, рассчитаем аппаратурные затраты для построения запоминающего устройства с 4-х разрядным кодом, сложность декодирующего устройства (элементов), зависимость достоверности (3) показана на рис.2.2.1. Для расчетов применяли алгоритм и программу:



Из таблиц видно, что лучшим из рассматриваемых вариантов является метод с кратностью ошибок от 0 до 3-х.

Используя выражения (1-3) рассчитаем и проведем оценку достоверности функционирования запоминающего устройства, работающего на основе предлагаемых подходов (см. табл. 2.2.4-7, рис.2.2.1).

Лучшие характеристики с точки зрения достоверности функционирования имеет устройство, построенное на основе первого метода.

Это объясняется использованием минимального количества простейших логических элементов для его построения.

Однако при этом процент обнаруживаемых и исправляемых ошибок у первого варианта (0-ошибок) – наименьший, а шестого (5-ошибок) – самый большой.

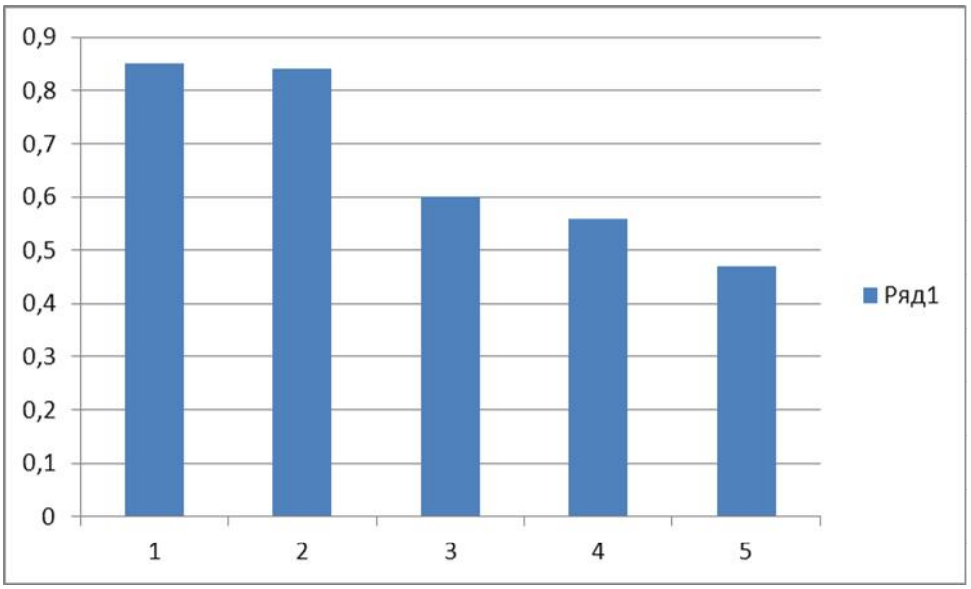


Рис.2.2.1. Зависимость достоверности от времени и от кратности ошибок:1-кратность 0-ошибок (ош); 2- 1ош; 3-2 ош; 4- 3 ош; 5- 4 ош; 6- 5 ош.

В результате, как это видно из табл.2.2.8 и формулы (2.2.4.) и рис.2.2.1., достоверность отказоустойчивых ЗУ улучшается в среднем на 70%.

Таблица 2.2.8. Достоверность ЗУ в СДО ТГУ во времени

Ошибки	2 сут	8сут	8 отн 2	Выигрыш во времени
Отсутствуют	0,96	0,95	0,99	
Одна Ошибка	0,96	0,8	0,83	0,85
Две Ошибки	0,96	0,8	0,83	0,84
Три Ошибки	0,95	0,8	0,84	0,84
Четыре Ошибки	0,9	0,54	0,6	0,6
Пять Ошибок	0,87	0,48	0,55	0,56
Шесть Ошибок	0,85	0,4	0,47	0,47

(0,85+0,84+0,84+0,6+0,56+0,47) / 6 = 0,69. (2.2.4)

2.3. Разработка информационной защиты СДО Йемена с криптографией

При проектировании защищенных СДО Йемена возникают проблемы выбора защиты (и бюджетной и эффективной). Одновременно это возможно

удовлетворить с помощью криптографии. Обоснуем и приведем разработанный нами подход, удовлетворяющий этим условиям. Предварительно проведем целевую классификацию для таких сетей[40,56-58,69,71].

Одна из основных задач криптографии — обеспечение конфиденциальности — связано с понятием шифрования.

Далее дадим краткое описание алгоритмов шифрования с использованием ключа, пригодные для структур, которые используются в СДО ТГУ (рис.2.3.1,2).

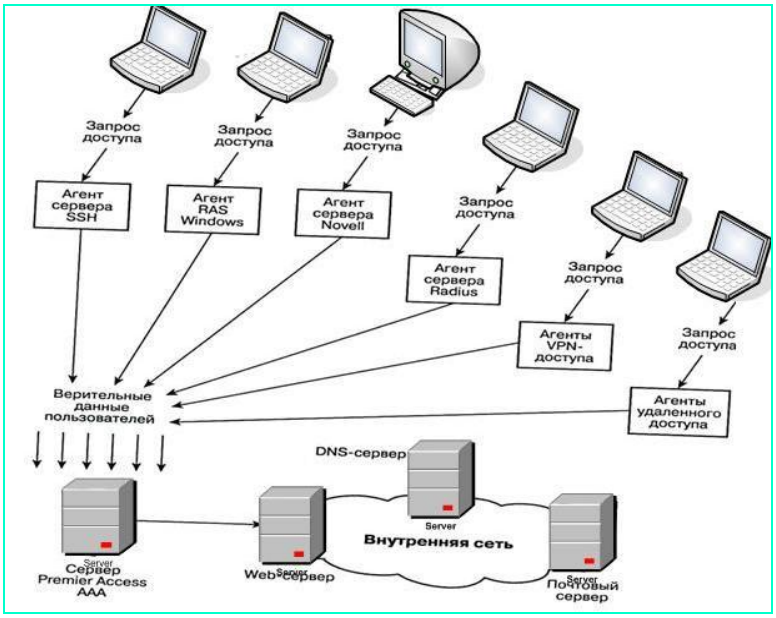


Рис.2.3.1. Структура внутренней сети СДО ТГУ

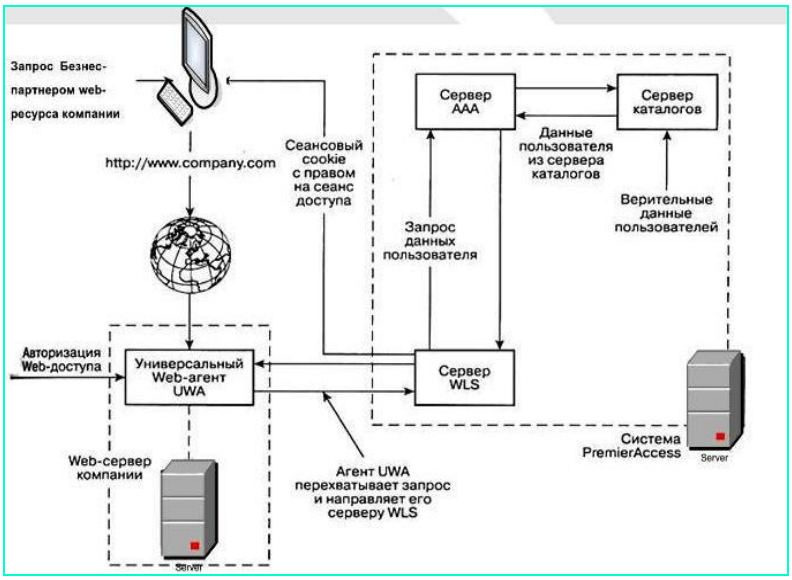


Рис.2.3.2. Структура внешних соединений СДО ТГУ

Алгоритмы шифрования могут быть разделены на два класса, в зависимости от того, какая методология криптосистем напрямую поддерживается ими. Алгоритмы шифрования с использованием ключей предполагают, что данные не сможет прочитать никто, кто не обладает ключом для их расшифровки [99,100].

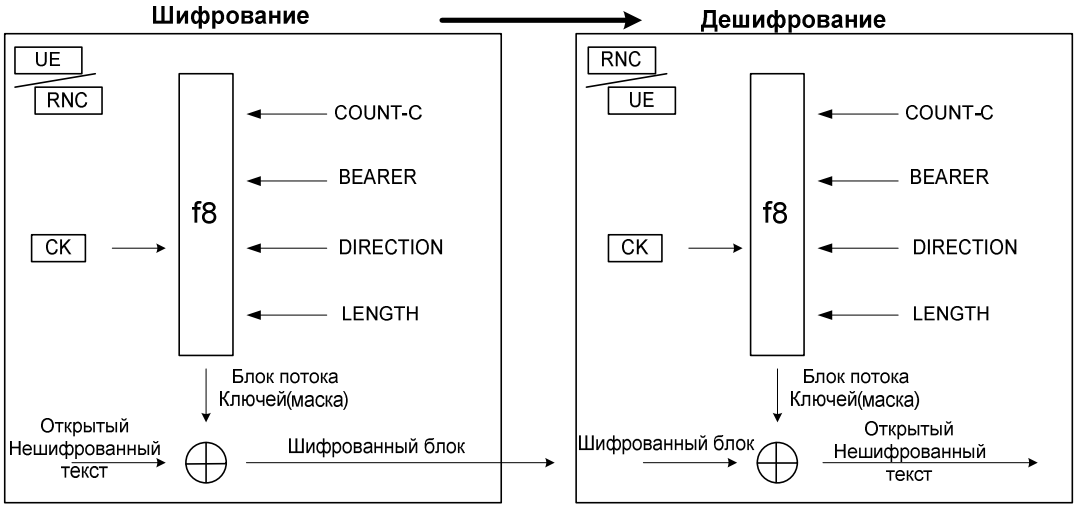


Рис.2.3.3.Механизмы шифрования/дешифрования в UMTS

Шифрование в универсальной мобильной телекоммуникационной системе (Universal mobile telecommunications system UMTS) происходит на втором уровне (L2), на уровне MAC (Media Access Control) или на уровне Radio Link Control (RLC). Точное местоположение функции шифрования зависит от типа соединения и контролируется высшими уровнями, именуемыми прозрачными RLC соединениями. Если трафик передается прозрачно через RLC, то шифрование происходит в уровне MAC. Для непрозрачных типов соединений это происходит в RLC уровне. Шифрование выполняется на индивидуальных логических каналах рис. 2.3.4.

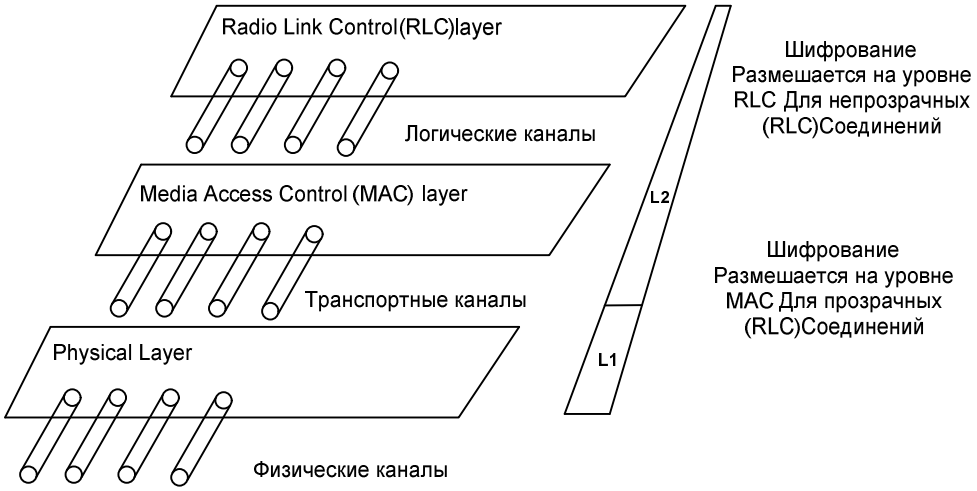


Рис. 2.3.4. Размещение функций шифрования на разных уровнях

Симметричные алгоритмы. (см. табл.2.3.1) [99,100].

Таблица 2.3.1. Структура шифрования

Тип	**Описание**	**Обеспечение**
DES (Data Encryption Standard)	Алгоритм шифрования: блок из 64 бит, используется 64-битовый ключ (требуется только 56 бит), 16 проходов.	Проект, администраи, пользователь
3-DES или тройной DES	64-битный блочный шифратор, использует DES 3 раза с тремя различными 56-битными ключами. Достаточно стоек ко всем атакам	Проект, администрация, пользователь
Каскадный 3-DES	Стандартный тройной DES, к которому добавлен механизм обратной связи, такой как CBC, OFB или CFB. Очень стоек ко всем атакам.	администрация, пользователь
FEAL	Блочный шифратор, используемый как альтернатива DES.	Проект, пользователь
IDEA	64-битный блочный шифратор, 128-битовый ключ, 8 проходов.	проект
Skipjack	64-битный блочный шифратор, 80-битовые ключи используются в режимах	Проект, пользователь

	ECB, CFB, OFB или CBC, 32 прохода	
RC2	64-битный блочный шифратор, ключ переменного размера.	Проект, пользователь
RC4	Потоковый шифр в 10 раз быстрее DES.	Проект, администрация, пользователь
RC5	Имеет размер блока 32, 64 или 128 бит, ключ с длиной от 0 до 2048 бит, от 0 до 255 проходов.	Проект, администрация, пользователь
CAST	64-битный блочный шифратор, ключи длиной от 40 до 64 бит, 8 проходов.	Проект, пользователь
Blowfish.	64-битный блочный шифратор, ключ переменного размера до 448 бит, 16 проходов.	Проект, администрация, пользователь
Устройство с одноразовыми ключами	Ключом (который имеет ту же длину, что и шифруемые данные) являются следующие 'n' бит из массива случайно созданных бит, хранящихся в этом устройстве.	Проект, администрация, пользователь

Асимметричные алгоритмы используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей [99,100] (см. табл.2.3.2).

Таблица 2.3.2. Таблица асимметричных алгоритмов

Тип	Описание	Обеспеченне	действие
RSA	алгоритм, факторизации	Проект	стойкость которого зависит от сложности факторизации больших целых

			чисел.
ECC (криптосистема на основе эллиптических кривых)	Использует алгебраическую систему, Его производительность на порядок выше, чем производительность RSA, Диффи-Хеллмана и DSA.	Проект, пользователь	описывается в терминах точек эллиптических кривых, для реализации асимметричного алгоритма шифрования
Эль-Гамаль.	Вариант Диффи-Хеллмана	пользователь	используется как для шифрования, так и для электронной подписи.

Порядок использования систем с симметричными ключами приведен нами в [99]

Асимметричная (открытая) методология. Один ключ делается известным всем, а другой держится в тайне. Приведем [99] следующие данные об эквивалентных длинах ключей:

Таблица 2.3.3. Длина ключей

Длина симметричного ключа	Длина открытого ключа	Задание и обеспечение
56 бит	384 бит	пользователь
64 бита	512 бит	пользователь
80 бит	768 бит	администрация пользователь
112 бит	1792 бита	администрация

		пользователь
128 бит	2304 бита	администрация пользователь

Порядок использования систем с асимметричными ключами проверенный и отлаженный нами[99] , в том числе при внедрении в ТГУ, Йемен (см. приложения):

Распространение ключей. Необходимо безопасное распространение ключа[99.100] апробированное нами (табл.2.3.4):

Таблица 2.3.4. Раздача ключей

Процедура	**Комментарии**	**Обеспечение**
Физическая раздача ключей	Используется как симметричными, так и асимметричными криптосистемами.	администрация пользователь
Выдача общего ключа участникам взаимодействия центром выдачи ключей	Может использоваться как симметричными, так и асимметричными криптосистемами. Так как при данном способе каждый пользователь должен каким-то образом безопасно взаимодействовать с центром выдачи ключей в самом начале работы, то это просто еще один случай, когда начальный обмен ключами является проблемой.	администрация пользователь
Предоставление центром сертификации ключей	Предоставление центром сертификации ключей доступа к открытым ключам пользователей и выдача секретных ключей	администрация

	пользователям	
Сеть доверия	Используется в асимметричных криптосистемах. Пользователи сами распространяют свои ключи и следят за ключами других пользователей	администрация пользователь
Метод Диффи-Хеллмана	Обмен секретным ключом по незащищенным каналам связи между двумя пользователями, которые до этого не имели общего секретного ключа. Уязвим к атаке "активное вмешательство в соединение".	пользователь

Изучив и апробировав вышеупомянутые методики, в компании ОАО «Ай-Ди Технологии Управления», нами [99,100] был выработан комплексный подход к защите информации в сфере электронного документооборота на платформе EMC Documentum и ее интеграцией с Системой Oracle IRM (в рамках реализации проекта по защите информации модуля «Конфиденциальная тайна» в АСУД (автоматизированная систему управления документооборотом) ОАО «ФСК ЕЭС»), который включает в себя использование криптографической шифрования документов, а так же использование электронного ключа eToken, как персональное средство авторизации, аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП).

Разработанное решение, позволило осуществить централизованное управление правами на документы, формирование контекстов документов КТ, в рамках которых задаются права доступа (табл.2.3.5):

Таблица 2.3.5. Права доступа

Процессы	**Ответственность**
Динамическое шифрование версий документа КТ	Администрация
Контроль доступа к набору (согласно классификации) или к любому конкретному документу, начала и конца доступа с возможность отмены права доступа в любой момент, того, как именно пользователи АСУД работают с документами на своих рабочих станциях	Администрация
Динамическое шифрование документов КТ при записи в репозитарий АСУД или когда они покидают его	Администрация, пользователь
Шифрование и снятие защиты, при движении документа по жизненному циклу в СЭД	пользователь
Полнотекстовая индексация документов КТ и версий, поиск по зашифрованным документам и версиям	Администрация, пользователь

Экспериментальная часть.

Цель: изучить аутентификации в сети GSM с использованием A3 алгоритма.

Теория:

Шифрование в сети GSM использует механизм запрос / ответ.

1. Мобильная станция (MS) признаки в сеть.

2. Подвижный центр службы коммутации (MSC) просит 5 троек из домашнего местоположения (HLR).

3. Регистр местоположения создает пять троек, использующих алгоритм A8. Эти пять троек содержат:

- 128-битный случайный вызов (RAND)
- 32-битная соответствия подписанный ответ (SRES)
- 64-битный ключ шифрования используется в качестве ключа сеанса (Кс)

4.Главная Регистрация местоположения отправляет центр переключения

мобильных услуг пяти троек.

5.Центр коммутации услуг мобильных посылает случайные вызов для базы передатчика станции (BTS).

6. Базовый передатчик станции отправляет случайный вызов от первой мобильной станции.

7.Мобильная станция получает случайный вызов от передатчика базовой станции и шифрует его с индивидуального ключа аутентификации абонен та (Ki) назначенного Мобильной станцией, используя алгоритм A3.

8. Мобильная станция посылает подписанный ответ приемопередатчика базовой станции.

9. Базовая приемопередающая станция посылает подписанный ответ на мобильный Центр услуг коммутации.

10. Мобильные услуги коммутационный центр проверяет подписанный ответ.

11. Мобильная станция генерирует сессионный ключ (Kc), используя алгоритм A8, Индивидуальный ключ аутентификации подписчика (Ki), назначенный для мобильной станции, и случайный вызов, полученных от приемопередатчика базовой станции.

12. Мобильная станция посылает ключ сеанса (Kc) с базовой станции.

13. Подвижный центр службы коммутации посылает сеансовый ключ (Kc) к передатчику базовой станции.

14. Базовая приемопередающая станция получает сеансовый ключ (Kc) от мобильной Услуги коммутационный центр.

15. Базовая приемопередающая станция получает сеансовый ключ (Kc) от мобильной Станции.

16. Базовая приемопередающая станция проверяет сеансовых ключей от мобильной станции и мобильный коммутационный центр услуг.

17. Алгоритм A5 инициализируется сессионным ключом, (Kc) и количество.

18. Канал связи между мобильной станцией и базой могут быть

зашифрованы с использованием алгоритма A5.

Считаем, наша методика пригодна при видах технологии атак, показанной на рис.2.3.5. и в предположении условий приведенных в табл.2.3.5.

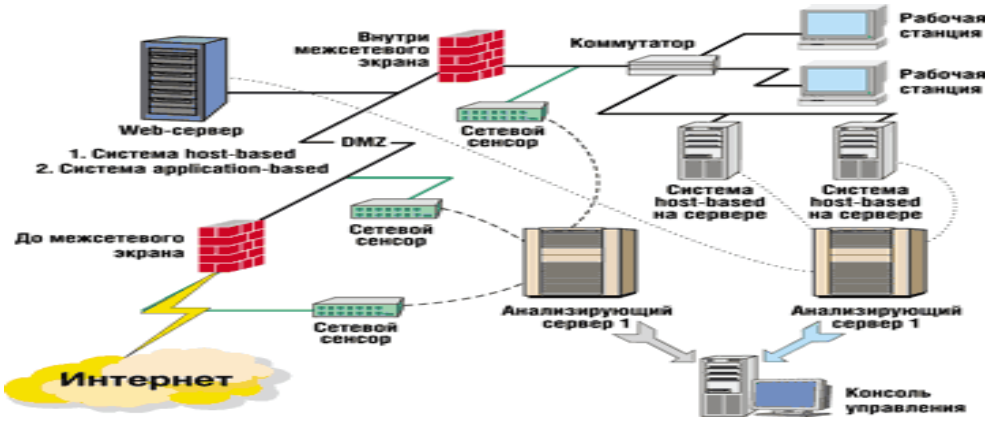


Рис.2.3.5. Технология обнаружения атак в сети

Таблица 2.3.5. Технологические возможности шифрования

Что могут и чего не могут системы шифрования	
Могут:	***Не могут:***
повысить защищенность сети; проводить мониторинг сетевого трафика за межсетевым экраном; проверять содержимое сетевого сообщения и определять тип атаки; выявлять изменения в файлах и директориях; выявлять необычное время и тип доступа к ресурсам.	обеспечить полную защищенность сети

Сравнение алгоритмов:

DES: (Data Encryption Standard), был первым стандартом шифрования. Он была разработана IBM на основе их Lucifer шифра. DES стал стандартом (www.tropsoft.com) и доступен для использования в Йемене[107]. DES использует 56 битовый ключ, и отображает 64-битный входной блок в 64 бит на выходе блока в. Ключ на самом деле выглядит 64 битным числом, но один бит в каждом из 8 октетов используется для нечетности на каждого октета.

AES: (Advanced Encryption Standard), а также известный как Rijndael - алгоритм, является симметричный блочный шифр, можно зашифровать

блоки данных 128 бит, используя симметричные ключи 128, 192 или 256. AES был введен, чтобы заменить DES. Атака полным перебором - единственным эффективным противоядием для этого алгоритма.

Blowfish: Blowfish является симметричный блочный шифр, которые могут быть эффективно использованы охраны данных. Это принимает ключ переменной длины, с 32 бит до 448 бит, что делает его идеальным для защиты данных[107].

Результаты выполненные нами при внедрении в ТГУ на машине, имеющей Intel® Core ™ i7-2600 (3,40 ГГц) процессор с Intel® Q65 Express 4 ГБ 1333 МГц DDR3 (RAM) и Ubuntu 12.04 Операционная система LTS. Платформа Java (openjdk1.6.0_14) используется для реализации. JCA (Java Cryptography Architecture) и JCE (Java Cryptography Extension) используются для шифрования реализации алгоритма. JCA является основной платформой, которая содержит «поставщик» архитектуру и набор API-интерфейсов для шифрования (симметричных шифров, асимметричных шифров, блочных шифров, потоковых шифров), сообщение дайджестов (хэш), цифровых подписей, сертификатов и проверки сертификатов, генерации ключей и обеспечить генерацию случайных чисел. Нами разработана структура для реализации криптографических алгоритмов.

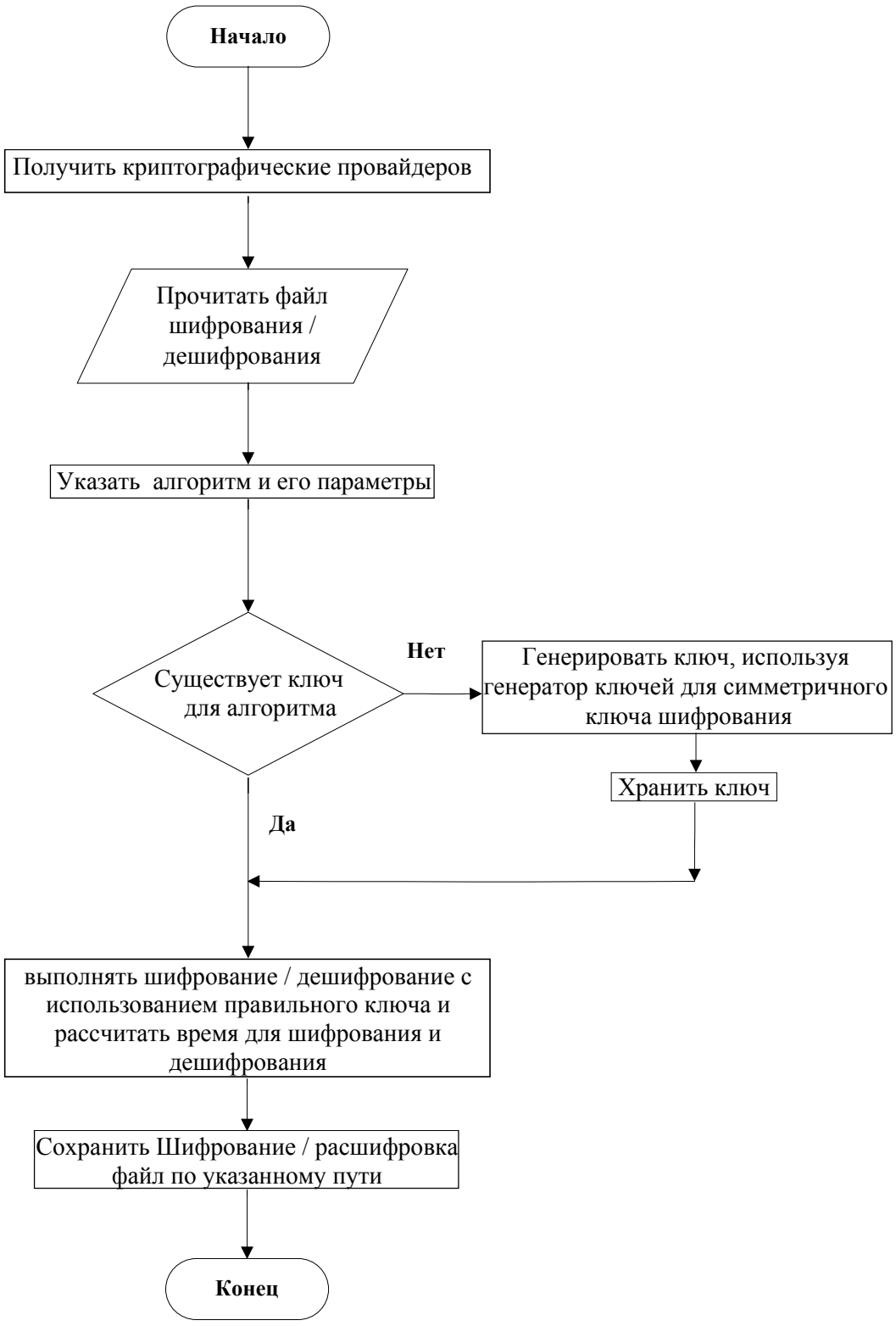


Рис. 2.3.6. Симметричная криптография (блок-схема алгоритма)

Блок-схема на рис.2.3.6 дает краткое представление о выполнении программы.

Программа проверяет, что ключ присутствует на алгоритме или нет. С генерированный ключ хранится по указанному пути. Таймер запускается

перед шифрованием или расшифровкой файла. Выходной файл записывается на указанное место. И результаты записываются. Экспериментальные результаты приведены на рис.2.3.7,8 для выбранных шести алгоритмов шифрования на другой метод кодирования. На рис.2.3.7 показаны результаты с основанием 64 кодирования, а на рис.2.3.8 приведены результаты шестнадцатеричной базы кодирование. Можно заметить, что нет существенной разницы в обоих способах кодирования. Те же файлы зашифрованы с помощью двух методов; мы можем признать, что две кривые почти дают одинаковые результаты.

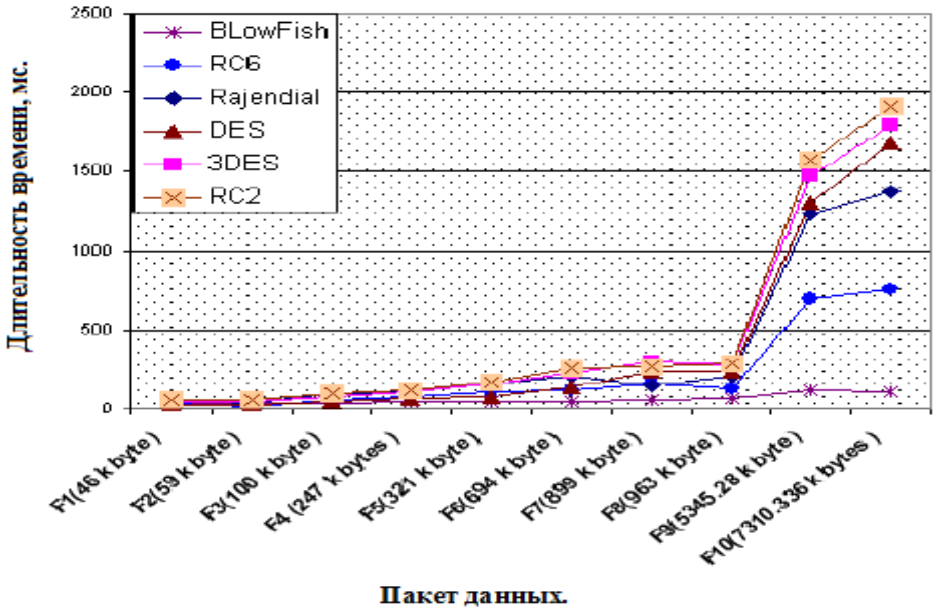


Рис.2.3.7. Время работы алгоритма шифрования(64 кодирование)

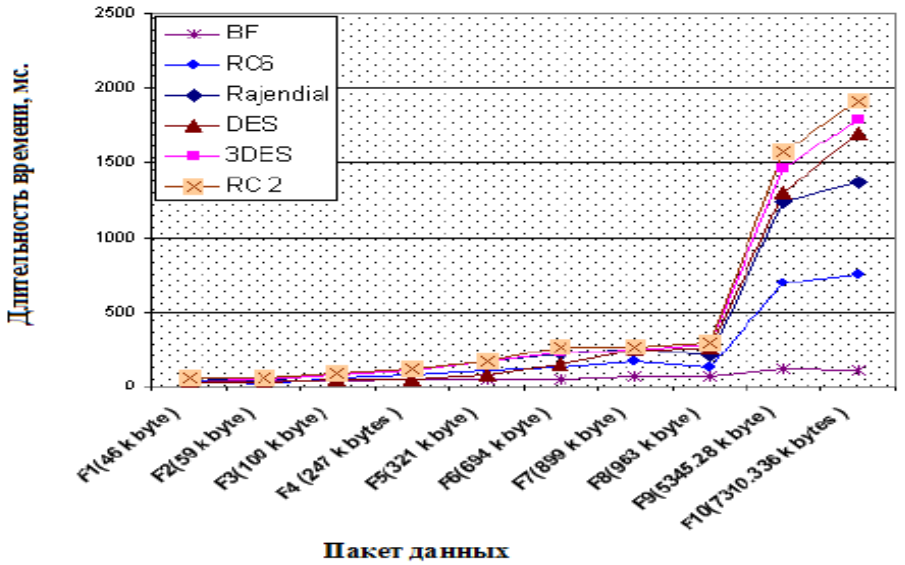


Рис.2.3.8. Время шифрования (в кодировании 16)

Время шифрования используется для расчета пропускной способности схемы

шифрования. Экспериментальные результаты показаны как гистограммы на рис.2.3.9 в стадии шифрования. Результаты показывают превосходство Blowfish алгоритма над другими алгоритмами с точки зрения времени обработки.

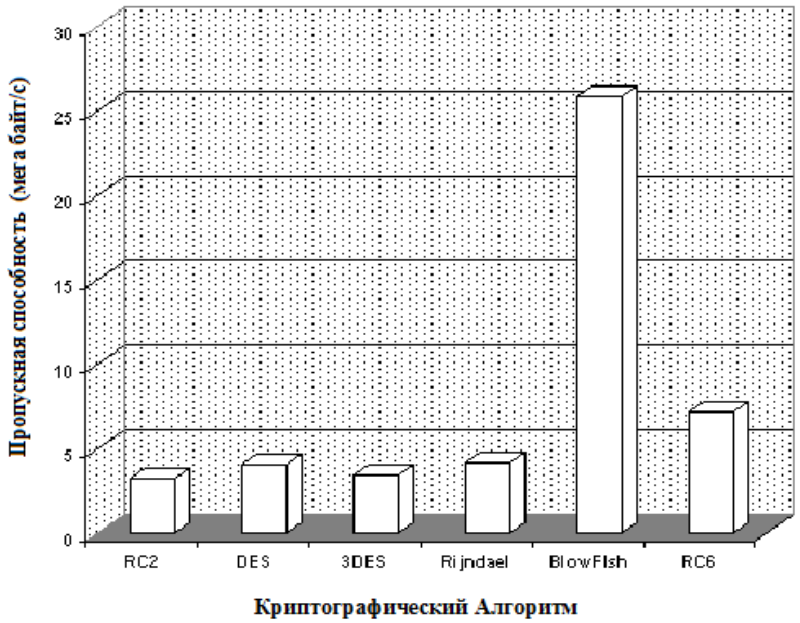


Рис.2.3.9. Пропускная способность каждого алгоритма шифрования (мб/с)

Таблица 2.3.6. Криптографические алгоритмы возможные для применения в Йемене [107]

Название алгоритма	Структура	Размер ключа (в битах)	Количество циклов	Тип шифрования
AES	Сеть подстановки с перестановкой	128, 192, 256	10, 12, 14	блок
DES	Сбалансированная сеть Фейстеля	56	16	блок
Triple DES	сеть Фейстеля	112, 168	48	блок
RC2	Сеть Фейстеля с тяжелым источником	40 - 1024	18	блок
Blowfish	Сеть Фейстеля	32-448	16	блок
Skipjack	несбалансированная сеть Фейстеля	80	32	блок
RC4	------	40-2048	256	поток

Разработанное нами решение[99,100], позволило осуществить централизованное управление правами на документы, формирование контекстов документов КТ, в рамках которых задаются права доступа, а именно:

1.Динамическое шифрование документов КТ при записи в репозитарий АСУД или когда они покидают его.

2.Динамическое шифрование версий документа КТ.

3.Полнотекстовая индексация документов КТ и версий, поиск по зашифрованным документам и версиям.

4.Шифрование и снятие защиты, при движении документа по жизненному циклу в СЭД.

5.Системный административный контроль:

-доступа к набору (согласно классификации) или к любому конкретному документу;

-начала и конца доступа с возможность отмены права доступа в любой момент;

-того, как именно пользователи АСУД работают с документами на своих рабочих станциях.

Таблица 2.3.6. Проникновения и сроки проектирования в сетях ТГУ и в СДО

Сети ТГУ	Известные технологии	использование наших методик	Время проектирования, дней	Число проникновений в месяц
«кадры»	«кадры»		9	15
«финансы»	«финансы»		6	7
«студент»	«студент»		10	21
«СДО»		«СДО»	3	2
«документооборот»	«документооборот»		12	8
«логистика»	«логистика»		15	11
«капитальное строительство»	«капитальное строительство»		12	7

При проведении эксперимента при внедрении (см. приложения) было замечено (см. табл.2.3.6), что число проникновений уменьшилось в 5 раз, а

время проектирования уменьшилось в 2,5 раза из-за целесообразного подбора ключей и их форматов применительно к сетям ТГУ по предложенному алгоритму и программе.

2.4.Архитектура безопасности GSM

•Аутентификация и согласование ключей

- Защита от несанкционированного доступа к услугам
- На основе алгоритма аутентификации A3 (Ki, RAND) → SRES

Он проверяет личность владельца смарт-карты, а затем решает мобильная станция допускается в конкретной сети. Количество (RAND) порождается алгоритмом с использованием секретного ключа Ki (128 бит)присвоенный этому мобильный телефон, шифрует RAND и посылает подписанный ответ(SRES -32 бит).СетьA3 SRES (32 bit) RAND Challenge (128 bit) Ki (128 bit) выполняет ту же процедуру SRES и сравнивает его значение с ответом, который он получил от мобильной таким образом, чтобы проверить, действителен ли секретный ключ, тогда аутентификации становится успешной, После аутентификации пользователя, ключ шифрования алгоритм генерирования A8(хранится в SIM-карте). Принимая RAND и Ki как входы, это приводит в ключе шифрования Кс, который передается для шифровки или расшифровки. Данные, это Кс (54 бит) используются с алгоритмом шифрования A5. Это Алгоритм содержится внутри аппаратных средств мобильного телефона таким образом, чтобы шифрования и расшифровки могли проходить в роуминге.

• Распределение и использование временных идентификаторов

- Запрет нарушителя от идентификации пользователей по IMSI
- Временное IMSI

Одним из примеров безопасности GSM с использованием нашего шифрования можно считать показанное на рис.2.4.1.

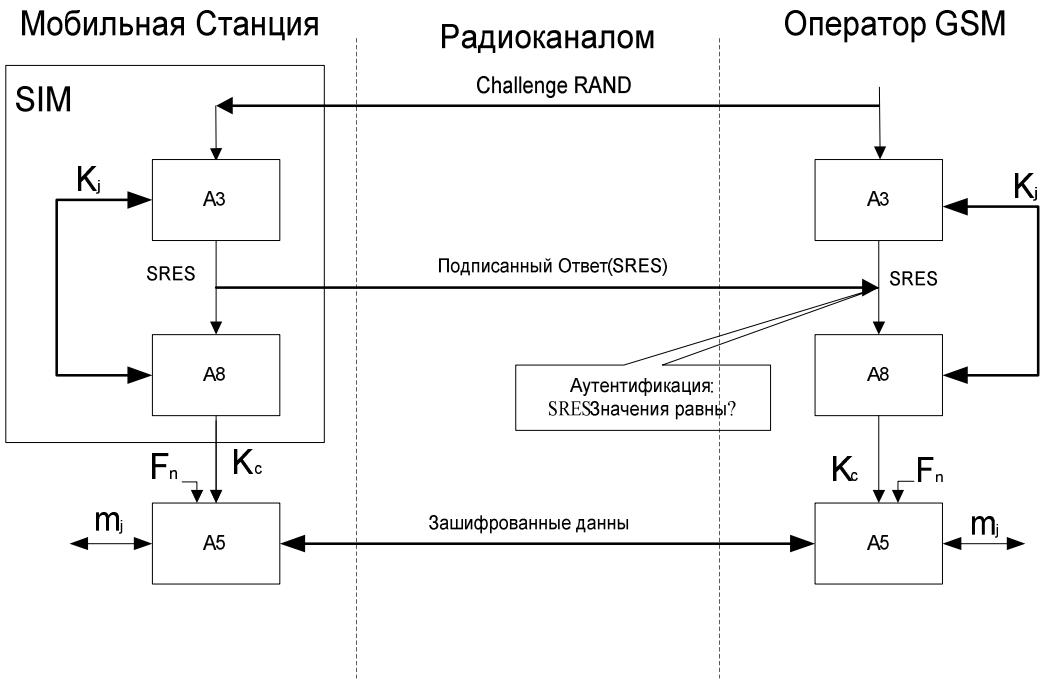


Рис.2.4.1. Обеспечение безопасности в GSM шифрованием

По этому показателю первое, что сеть должна сделать, это идентификации и аутентификации клиента. Для этого сеть передает 128 бит вызов на телефон клиента.

SIM в телефон, то используется алгоритм A3 и отдельного абонента ключей аутентификации (Ki, уникальное для каждого различного SIM), чтобы вычислить подписанный ответ (SRES) и отправляет его обратно к базовой станции. Здесь SIM-использует другой алгоритм, A8, Ki и исходный вызов, чтобы вычислить сеансовый ключ (Kc) и посылает это к базовой станции. Этот ключ сеанса в настоящее время используется вместе с алгоритмом A5 для шифрования данных.

Аутентификация требуется в каждом мобильной системе радиосвязи:

- Чтобы установить подлинность пользователя / оборудования.
- Выяснение, разрешено ли пользователю для доступа к услуге.
- Аутентификации состоит из запроса и ответа.
- Сеть представляет собой систему в виде случайных чисел RAND.
- Ответ SRES выводится на основе алгоритма A3 с проблемой (RAND),ключ аутентификации Ki и IMSI.

MS отвечает на вызов, отправив SRES обратно в сеть, которая сравнивает

SRES MS с его собственными SRES (см. рис.2.4.2).

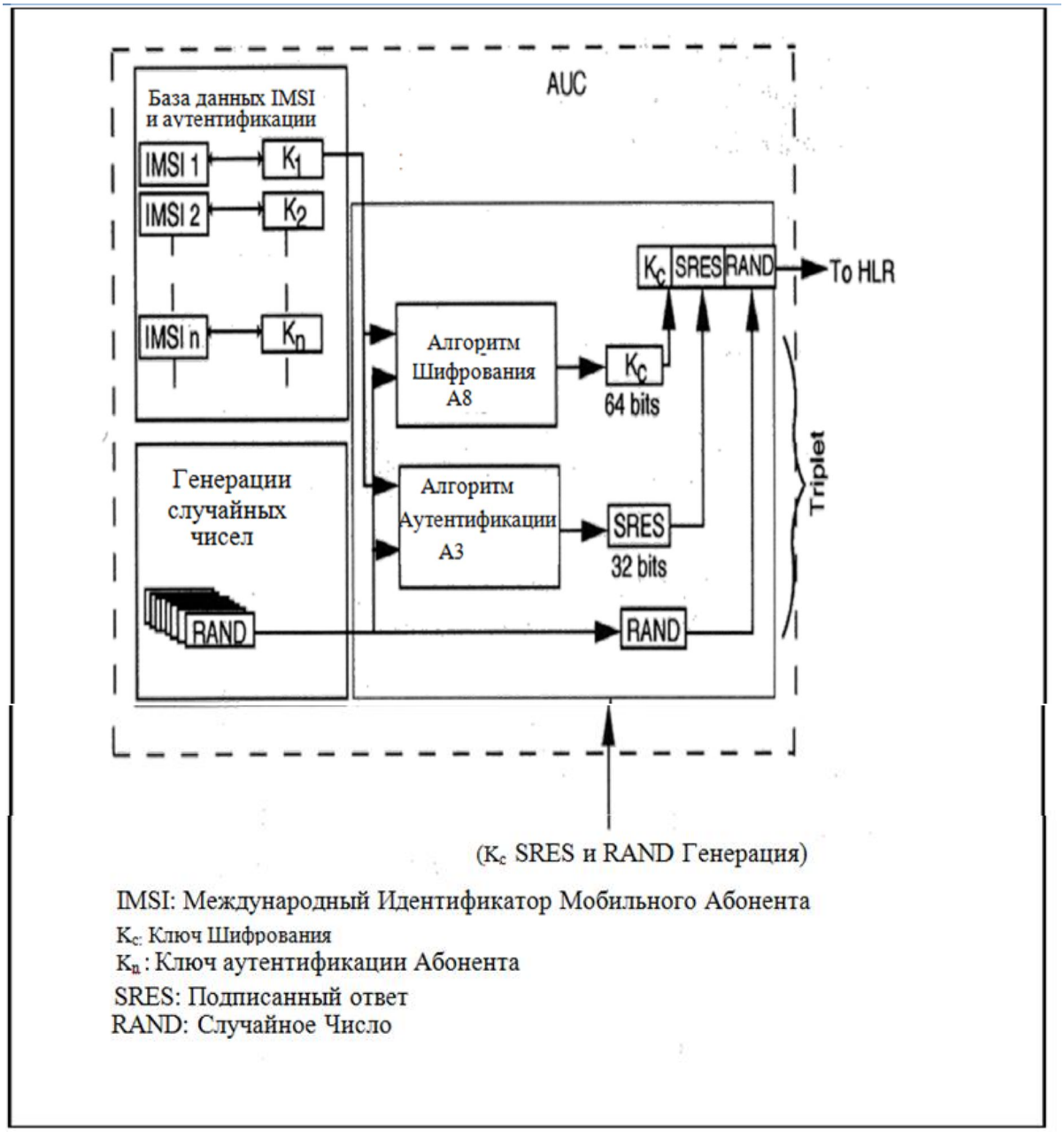


Рис.2.4.2. Генерация тройки

Шифрование

 Защита аналоговой информации от перехвата.

Описание: Аутентификация GSM и шифрование есть применение многих вводов / выводов, как показано на рис.2.4.2. Первоначально Запрос аутентификации направляется в систему, и ответ аутентификации приходит в качестве выходного сигнала.

Экспериментальный анализ:

1.MS аутентификации на основе его IMSI номер на сервере MSC.-

2.Случайное число будет создаваться на AUC и будет предоставляться MC, Где в нем можно использовать это случайное число наряду с Ki производить SRES с использованием алгоритма A3.

3. так же, SRES будет генерироваться в HLR и оба SRES будет проверяться на MSC для аутентификации пользователя.

4. Kc, шифрование ключ будет создан алгоритм A8, используя случайныечис ла и Ки в качестве входных параметров.

5. Kc будет использоваться в качестве ключа шифрования для A5 алгоритм для шифрования голосовых данных через эфир.

Экспериментальные шаги:

Запуск сервера MSC:./ serverexe 127.0.0.1 1024

Он будет ждать, чтобы получить номер IMSI мобильной станции (рис.2.4.3)

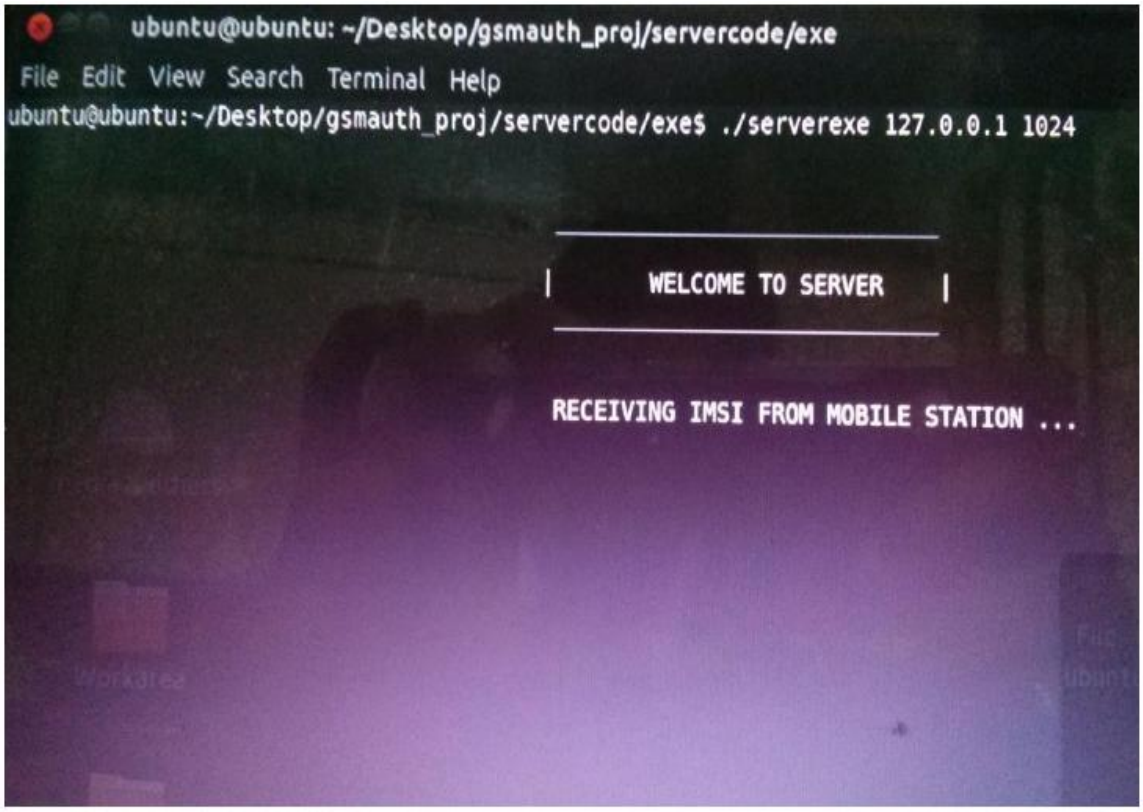
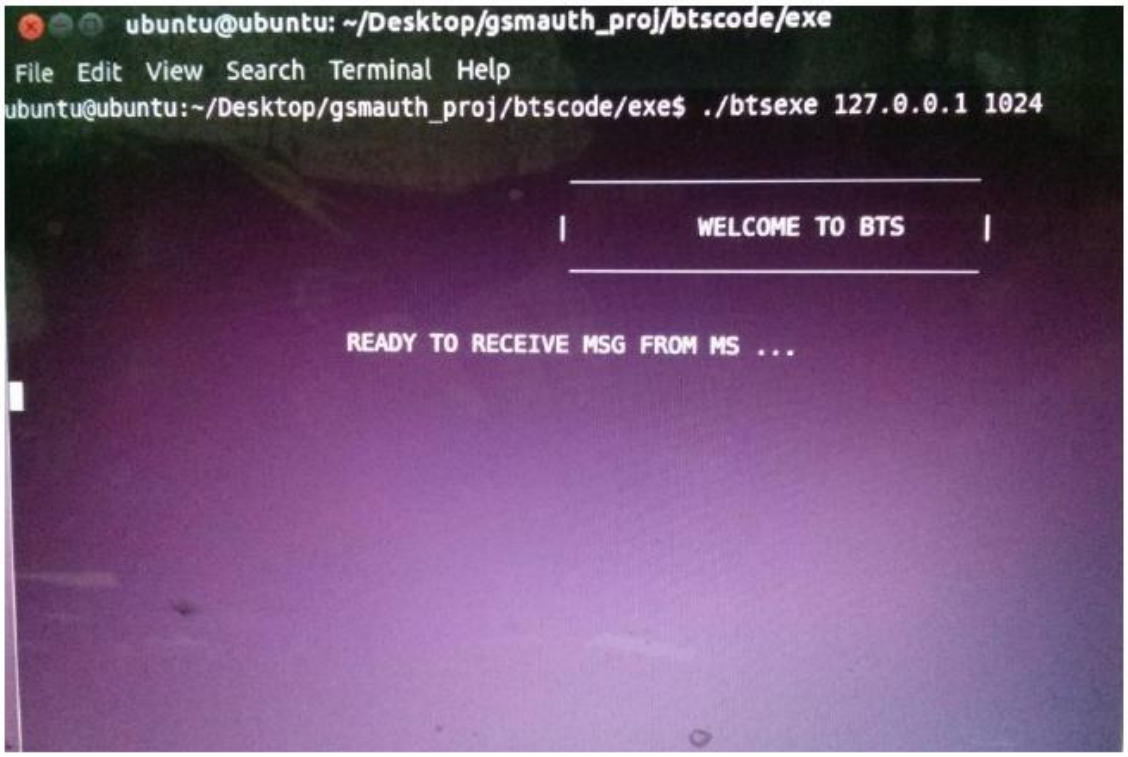


Рис.2.4.3. Ожидание номера.

Начало BTS:. /
btsexe 127.0.0.1 1024Он будет получать сообщение от MS и расшифровывать его (рис.2.4.4).



Начать MS: ./clientexe 127.0.0.1 1024 127.0.0.1 1025

Он пошлет IMSI на сервер MSC и как только аутентификация выполняется, он может начать отправку сообщений BTS с помощью алгоритма A5.

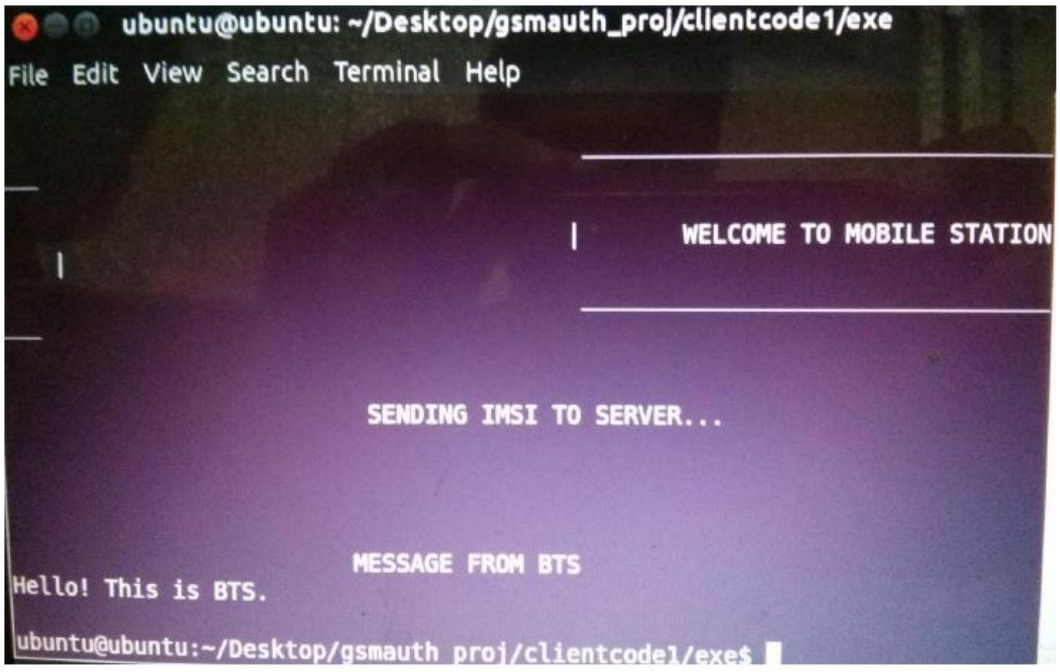


Рис. 2.4.4. Расшифровывание

Аутентификация: MSC получает IMSI от MS и подлинность его (рис.2.4.5).

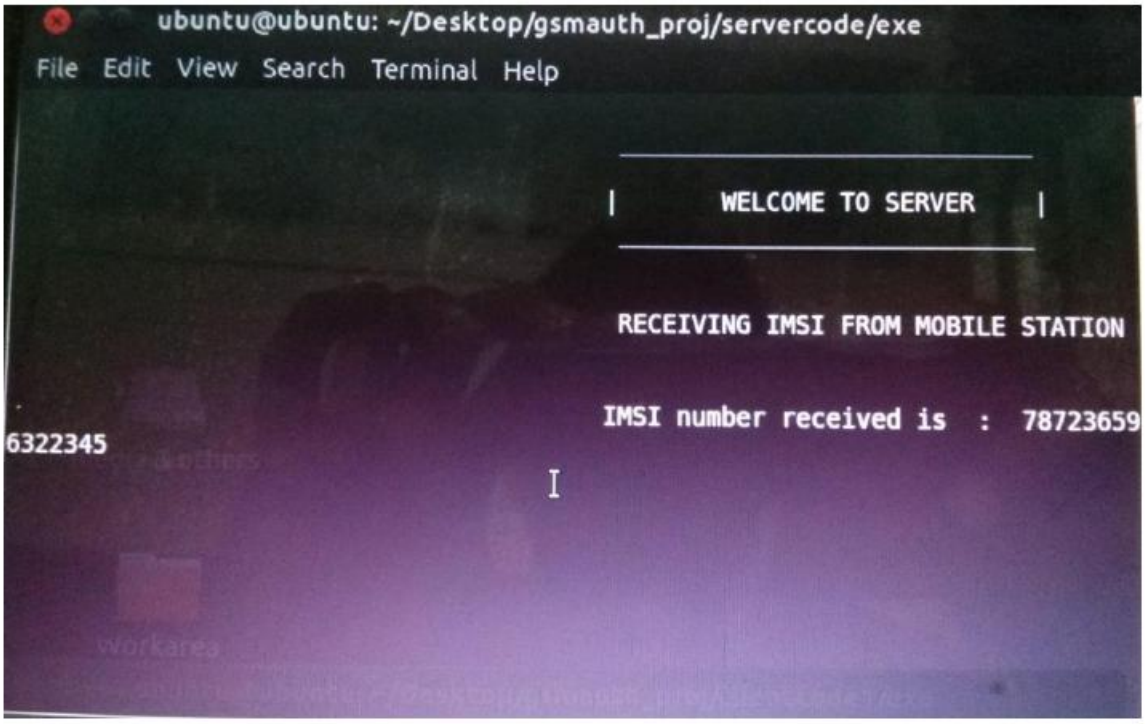


Рис.2.4.5. Подлинность

Сообщение, полученное по BTS от MS с помощью алгоритма A5 для расшифровки зашифрованного сообщения от MS. Один MSC и BTS может взаимодействовать с несколькими MC (рис.2.4.6).

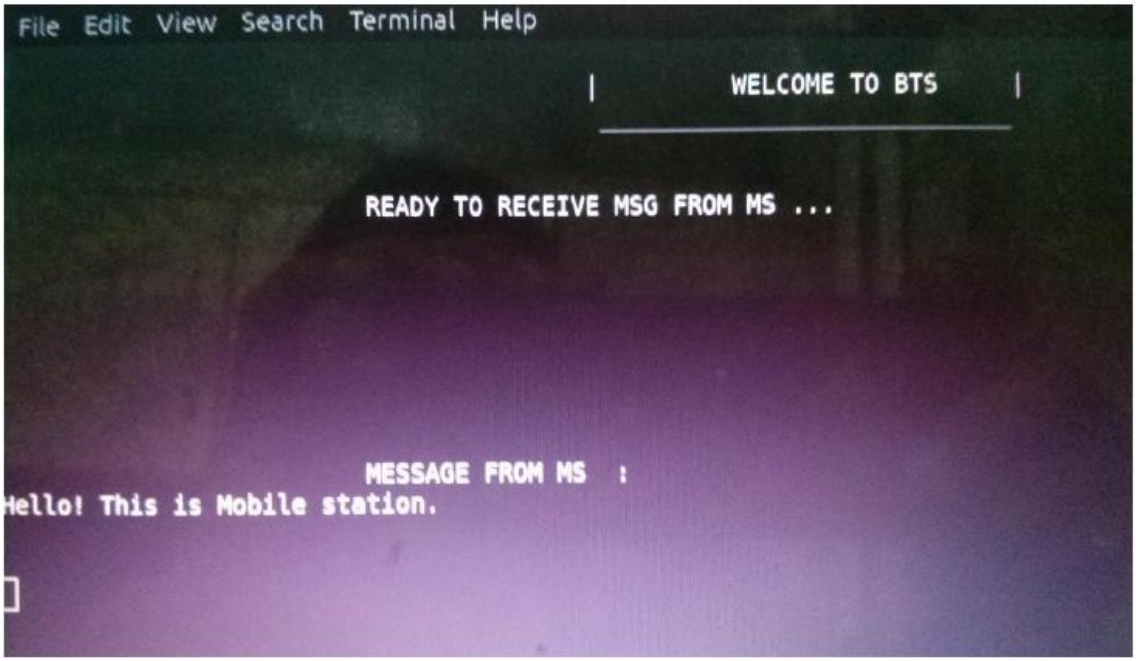


Рис.2.4.6. Сообщение

Аутентификация на MSC: MSC получает IMSI от MS и аутентифицирует его (рис.2.4.7).

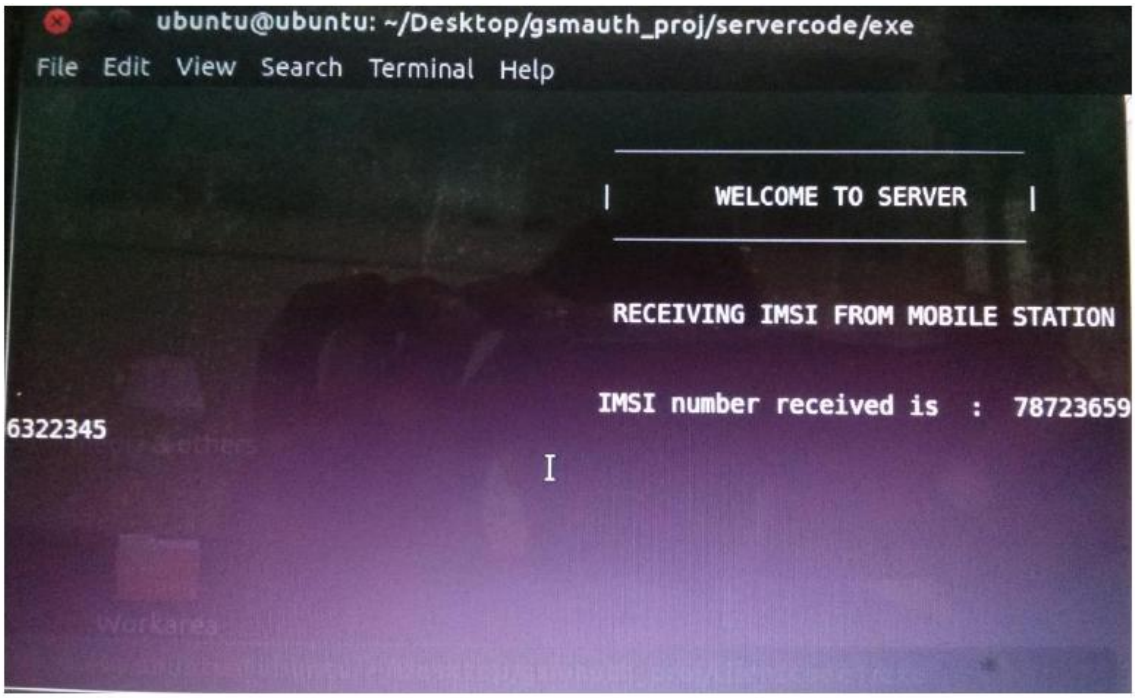


Рис.2.4.7. Аутентификация

Внедрение этих наших разработок в сетях СДО ТГУ позволило уменьшить количество несанкционированных проникновений в 5 раз, не добавляя дополнительно аппаратных устройств и незначительно меняя структуру (см. приложения).

2.5. Улучшение информационной безопасности в GSM при использовании в СДО Йемена

Подробнее об особенностях республики Йемен см. прилож. 1 Приведем разработанный нами подход к защите информационной безопасности СДО при использовании каналов с GSM на примере сети ТГУ (Йемен) с использованием модулей (см. табл.2.5.1).

Таблица 2.5.1. Модули и каналы GSM

модули	название	Действие
SIM, Smart-card	Subscriber Identity Module	съемный модуль, вставляемый в соответствующее гнездо

		абонентского аппарата
PIN	Personal Identification Number	международный идентификатор абонента подвижной связи (International Mobile Subscriber Identity — IMSI)
TMSI	Temporary Mobile Subscriber Identity	временный идентификатор абонента подвижной связи, присваиваемым аппарату при его первой регистрации в конкретном регионе
LAI	Location Area Identity	идентификатор местоположения и сбрасываемым при выходе аппарата за пределы этого региона

Процедура аутентификации стандарта GSM схематически показана на рис.2.5.1.

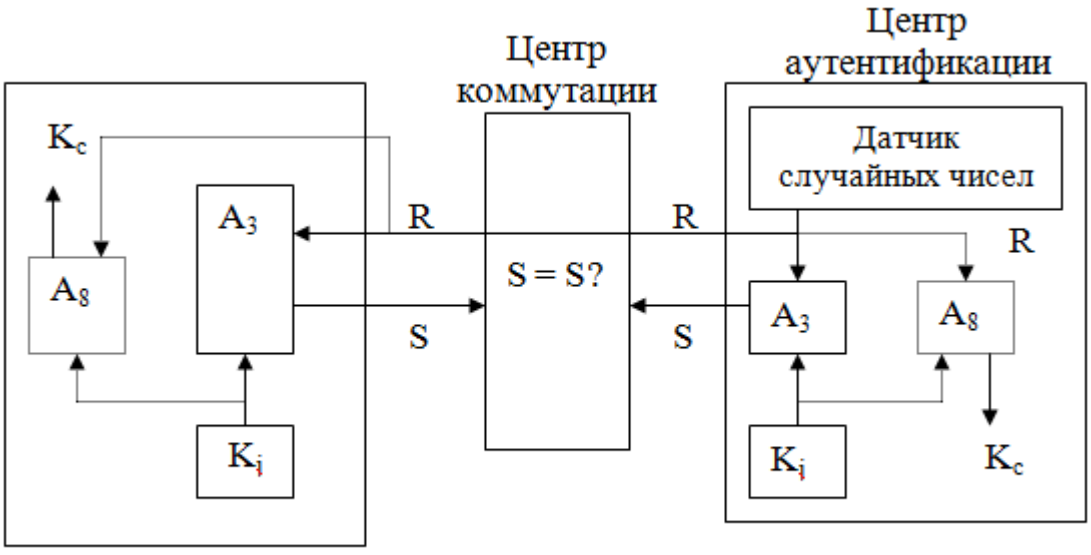


Рис. 2.5.1. Схема процедуры аутентификации в стандарте GSM: — случайное число; A3 — алгоритм аутентификации; A8 — алгоритм вычисления ключа шифрования; Ki — ключ аутентификации; Kc — ключ шифрования; S — зашифрованный отклик(SignedResponse-SRES).

Пунктиром отмечены элементы, не относящиеся непосредственно к процедуре аутентификации, но используемые для вычисления ключа шифрования Кс. Вычисление производится каждый раз при проведении аутентификации.

Процедура идентификации заключается в сравнении идентификатора абонентского аппарата с номерами, содержащимися в соответствующих «черных списках» регистра аппаратуры, с целью изъятия из обращения украденных и технически неисправных аппаратов. Идентификатор аппарата делается таким, чтобы его изменение или подделка были трудными и экономически невыгодными.

Работа по обеспечению секретности GSM ведется в 3GPP и существуют разные подходы к уровню секретности, который следует применять. Одно предложение - шифрование должно защищать практически все интерфейсы (сигнализации и пользовательских данных). Другое предложение - шифровать только важные пользовательские данные (например, ключи шифрования) в процессе роуминга между разными сетями.

На рис.2.5.2 представлена архитектура обеспечения секретности в сетях 3G, как определено для версии 4.

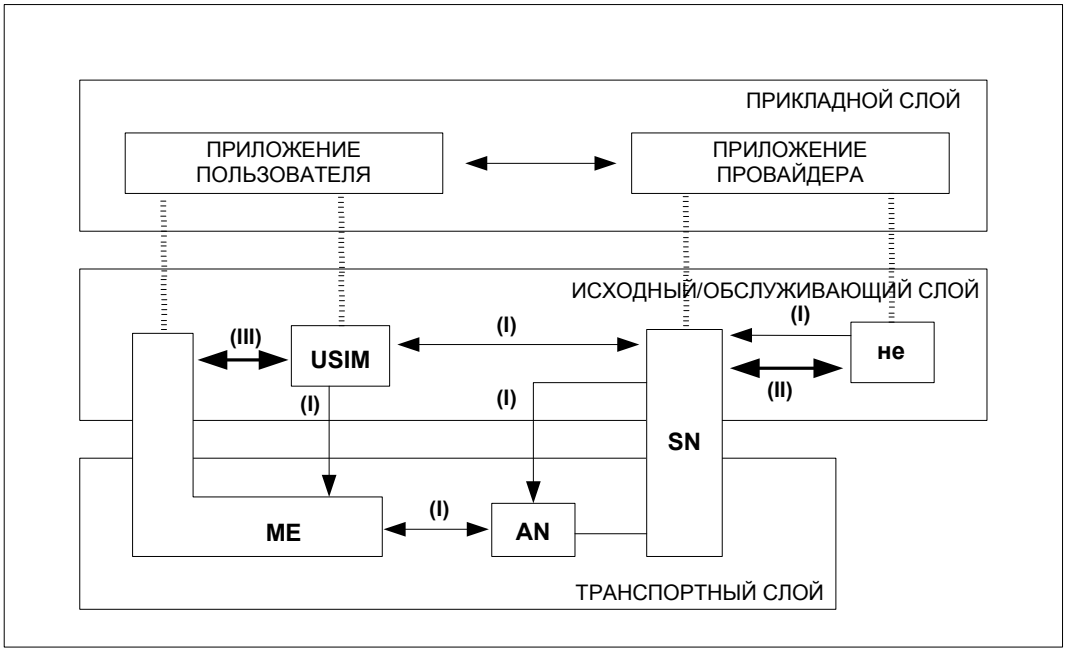


Рис.2.5.2.Обзор архитектуры обеспечения секретности в 4-й верси

Выводы по главе 2

1. Рассмотрены методики и устройства для поиска несанкционированных проникновений в телекоммуникации в том числе и в СДО.
2. Приведены основные проблемы защиты информации в GSM применительно к СДО Йемена.
3. Предложена методика повышения достоверности защищенных запоминающих устройств на 70%.
4. Проанализированы основные особенности защиты информации применительно к республике Йемен на примере ТГУ и разработаны подходы для улучшения эффективности защиты СДО при использовании криптографии и при использовании GSM. При этом число проникновений уменьшилось в 5 раза, что нами установлено при внедрении (см. приложения).

Глава 3.Оценка целесообразности организации защиты информации от несанкционированного доступа в СДО Йемена

3.1. Угрозы. Проникновения и защита от них. Эффективность защитных мероприятий в СДО

Для каждого типа угроз может быть одна или несколько мер противодействия[54,55,89,90,106,107].

Взаимосвязь различных видов угроз безопасности информации с видами нарушений и последствий, к которым они приводят, представлены на рис. 3.1.1.

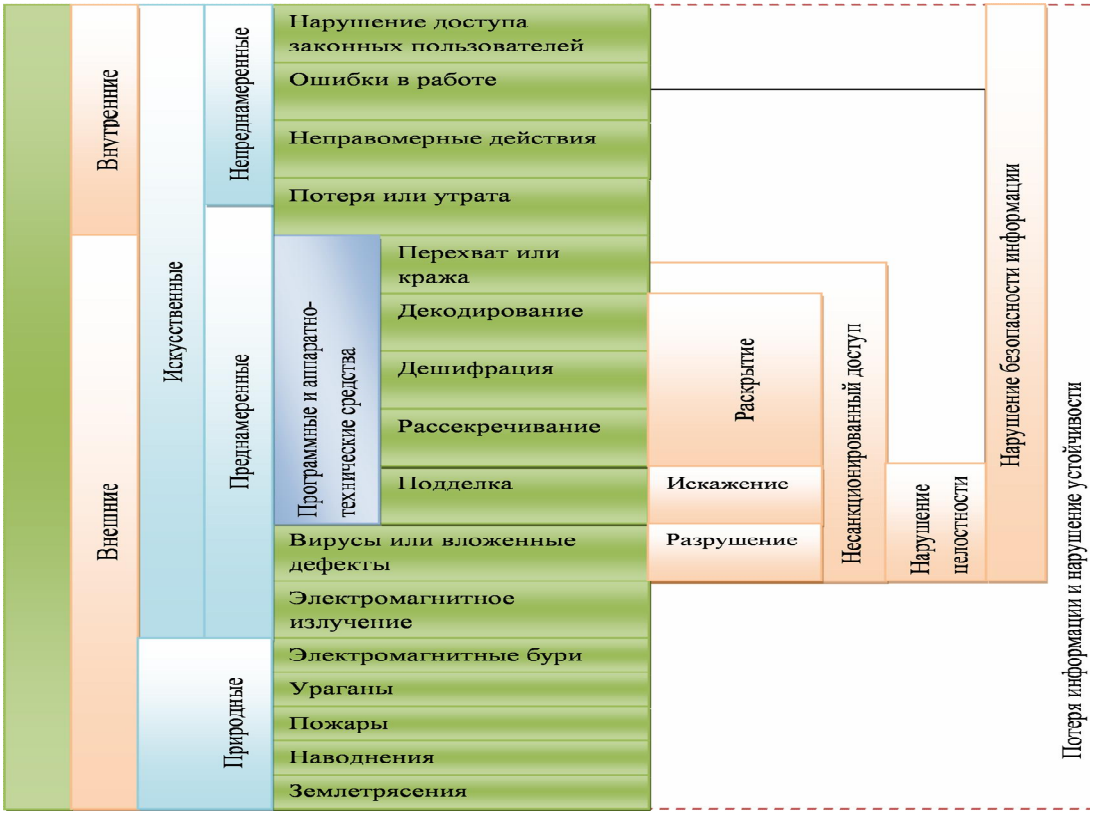


Рис. 3.1.1. Виды угроз, влияющие на безопасность информации и устойчивость функционирования ТКС

Решение проблемы обеспечения безопасности информации в сетях передачи данных должно осуществляться системно на основе оценки эффективности защиты информации, передаваемой по каналам связи, и не должно рассматриваться как чисто техническая задача, которая может быть решена попутно с разработкой элементов сети.

В связи с неоднозначностью выбора мер противодействия в СДО необходим поиск некоторых критериев, в качестве которых могут быть использованы

надежность обеспечения сохранности информации и стоимость реализации защиты. Принимаемая мера противодействия будет приемлема, если эффективность защиты с ее помощью, выраженная через снижение вероятного ущерба, превышает затраты на ее реализацию. В этой ситуации можно определить максимально допустимые уровни риска в обеспечении сохранности информации и выбрать на этой основе одну или несколько обоснованных мер противодействия, позволяющих снизить общий риск до такой степени, чтобы его величина была ниже максимально допустимого уровня. Из этого следует, что потенциальный нарушитель, стремящийся рационально использовать 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 и телекоммуникаций СДО рассматривают любой механизм защиты как некоторые дополнительные затраты с желанием за их счет снизить общие расходы(время, деньги, скорость и т.п.)[54,55]. При решении на уровне руководителя проекта вопроса о разработке средств защиты необходимо учитывать соотношение затрат на реализацию процедуры и достигаемого уровня обеспечения сохранности информации. Поэтому разработчику нужны методики, связывающие уровень защиты и затраты на ее реализацию, которые позволяли бы определить затраты на разработку потребных средств, необходимых для создания заранее определенного уровня защиты. В общем виде такую зависимость задают исходя из следующих соображений.

Защита требует особых подходов и к аппаратному построению телекоммуникаций и к программным решениям. Можно выиграть в защите от проникновений или в защите от предполагаемых угроз в виде повышения эффективности защитных мероприятий, и при этом потерять в скорости или

получить существенное увеличение затрат на разработку, изготовление и/или на дорогое программное обеспечение.

Следовательно, нам необходимо получить оценки эффективности мероприятий по защите корпоративных сетей СДО Йемена от несанкционированного доступа при учете большинства национальных особенностей (см. приложения1, 2, 3, акт внедрения).

Ранее было отмечено, что наиболее достоверные критерии эффективности при защите от НСД – технико-экономические или другие, которые учитывают затратные механизмы проектов. При оценке необходимости защиты предприятия от несанкционированного доступа к информации можно считать, что полные затраты (потери) уменьшаются[54,55,106,107].

Рассмотрим моделирование информационных каналов СДО для целей защиты и его адекватность, зависимость эффективности от срывов и влияние различных факторов на защищенность.

3.2. Оценка адекватности моделирования информационного канала СДО

Рассмотрим известные и возможные критерии эффективности моделирования (ЭМ)[55,94-96,106]:

$$\max \text{Эм} = \frac{\text{П}_{\Sigma}}{\text{З}_{\text{с}} + \text{З}_{\text{экс}}} \qquad (3.2.1)$$

$$\max \left\{ \text{П}_{\Sigma} \right\} \Big/ (\text{З}_{\text{с}} + \text{З}_{\text{экс}}) \le \text{З}_{\text{с}} \qquad (3.2.2)$$

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

$$\frac{\max\{\mathit{П}_{\Sigma}\}}{\min\{\mathit{Зс} + \mathit{Зэкс}\}} \qquad (3.2.4)$$

1. $Эм = \frac{\sum_{i=1}^{S} n_i q_i L_i}{\sum_{i=1}^{S} n_i L_i}$, или если $C_i = n_i L_i$; $C = \sum_{i=1}^{S} n_i L_i = \sum_{i=1}^{S} C_i$, то

2. $Эм = \frac{\sum_{i=1}^{S} q_i C_i}{C}$,

$q_i = \frac{p_i}{p_{iб}}$

3. $Эм = \frac{\sum_{i=1}^{S} \alpha_i q_i C_i}{\sum_{i=1}^{S} C_i}$, $\sum_{i=1}^{S} \alpha_i = 1$,

где α_i– коэффициент важности («веса») i-го параметра[55].

Стоимость (затраты) могут выражаться в различных единицах (аппаратные, денежные, временные, количество студентов и тьюторов и т.п.).

Индексные показатели можно использовать для оценки общей эффективности нескольких моделей СДО. Их можно использовать в инженерных субоптимизациях[55].

$Ик = \frac{\sum_{i=1}^{S} n_i q_i L_i}{\sum_{i=1}^{S} n_i L_i}$, $C_i = n_i L_i$, $C = \sum_{i=1}^{S} n_i L_i = \sum_{i=1}^{S} C_i$, $Ик = \frac{\sum_{i=1}^{S} q_i C_i}{C}$,

$Икобщ = \frac{C1 Ик1 + C2 Ик2 + ... + Cm Икm}{C1 + C2 + ... + Cm} = \frac{\sum_{j=1}^{l} C_j Икj}{\sum_{j=1}^{l} Cj}$,

$Ки = \frac{П_{\Sigma}}{З_с + З_{ПП}}$, $Э = \frac{\sum_{i=1}^{S} \alpha_i q_i C_i}{\sum_{i=1}^{S} C_i}$, $\sum_{i=1}^{S} \alpha_i = 1$.

Разработанная методика был применена для расчета показателей качества компьютерных классов ТГУ (Йемен). Предлагаем расчеты.

Возможно будет важнее не адекватность модели соответствующей

конкретной СДО (точность соответствия) по одному или группе параметров, а затраты на моделирование (время, средства и т.п.) или эффективность конкретной СДО.

Описание конкретной СДО, когда ее сетевая структура неизвестна, формируется с помощью подбора соотношений[55].

$$Эм = \frac{\sum_{i=1}^{S} n_i q_i L_i}{\sum_{i=1}^{S} n_i L_i};$$

$$Эм = \frac{\sum_{i=1}^{S} \alpha_i q_i C_i}{\sum_{i=1}^{S} C_i};\ \sum_{i=1}^{S} \alpha_i = 1.$$

Нами при внедрении в ТГУ были проведены расчеты, приведенные в табл.3.2.1.

Таблица 3.2.1. Индексные показатели с учетом эффективности и затратных мероприятий для классов ТГУ, рассчитанные по методике [55], с использованием наших алгоритма и программы.

	Компьютерные классы ТГУ				
параметры	КК химии	КК биологии	КК психологии	КК информатики и защиты информации	множитель
λi , 1/ч	1	0,5	2	0,8	0,01
T_{bi}, ч	2	4	6	2	0.1
$T_{усi}$, ч	1,6	1	4,8	1,4	0,1
g_{1i}, усл.ед.	10	20	10	30	-

g_{2i}, у с л . е д .	5	10	20	20	-
Индексный показатель	0,3	0,6	0,5	0.86	-

При анализе табл. 3.2.1, становится понятным, что в наилучшем положении находится класс информатики и защиты информации, поскольку в нем первоначально было исследовано и внедрена разработанная методика (см. приложения)

При исследовании телекоммуникационной сети СДО математическим моделированием применяются все способы идентификации. Это нами проверено при внедрении в СДО ТГУ.

Для сравнения разных подходов, при разных параметрах, при применении этой расчетной методики, нами разработан алгоритм (рис.3.2.1).

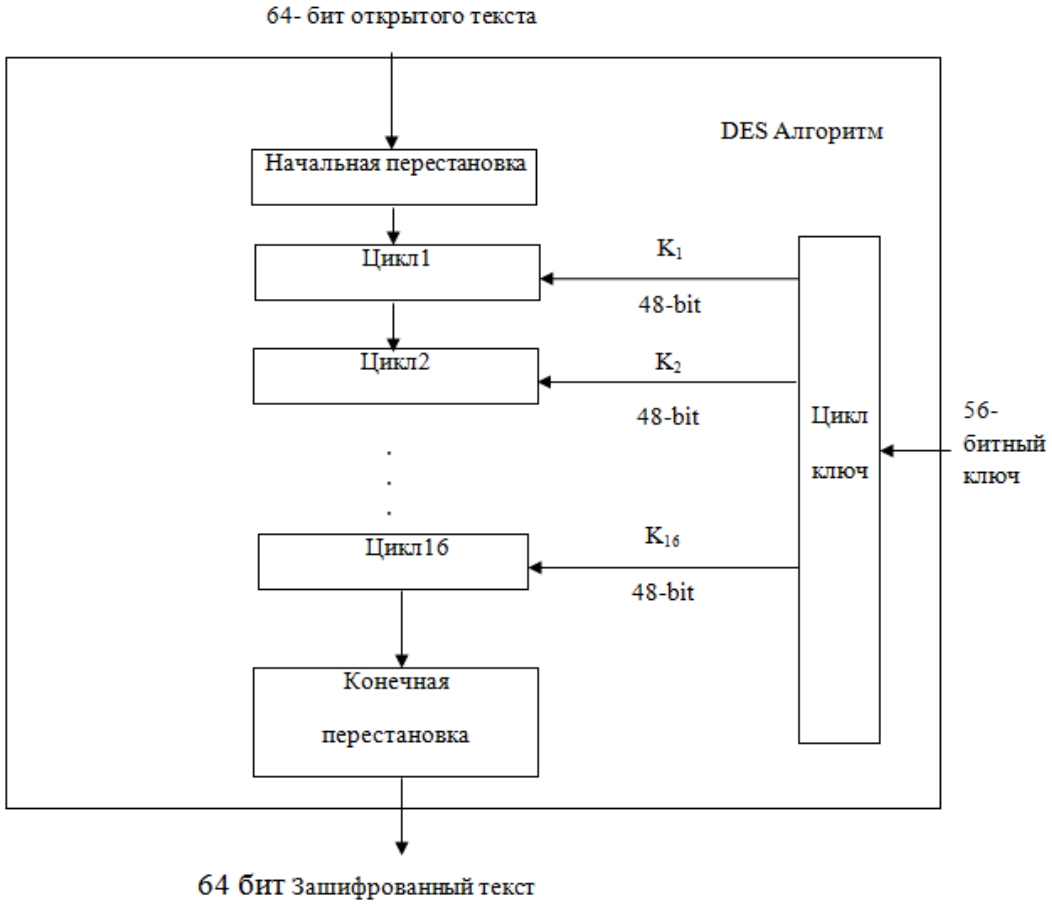


Рис.3.2.1. Сравнительный алгоритм.

Приведем временные данные для разных алгоритмов (табл.3.2.5,6).

Таблица 3.2.5. Время выполнения шифровки (мс) для разных пакетов данных

Входной размер(кб)	3 DES	DES	RSA
45	50	25	55
55	44	29	46
96	76	45	89
236	113	79	119
319	155	89	157
560	177	131	179
899	299	240	369
5345.28	1166	1296	1441
Пропускная способность (мб / с)	2.08	3.01	1.67

Таблица 3.2.6. Время выполнения (мс) расшифровки для разных пакетов данных

Входной размер (кб)	3DES	DES	RSA
45	45	36	55
55	42	31	48
96	65	49	73
236	104	88	105
319	135	89	157
560	160	131	169
899	181	152	173
5345.28	845	785	880
Пропускная способность (Мб / с)	4.03	5.012	2.147

Эта расчетная методика и приведенные таблицы позволяют выбрать наилучшие стратегии защитных мероприятий в разных случаях.

3.3.Зависимость эффективности сети СДО от срывов

Эффективность систем связи зависит, в частности, от количества и длительности срывов связи между различными абонентами и центрами[55,104,107]. В сложных системах связи (сетевых), к которым относится и СДО, большое значение имеет установление зависимости

эффективности сети от срывов.

Рассматриваемая сеть СДО состоит из N абонентов, между i – м и j – м из которых возможна связь через определенное число каналов Kl (l – число абонентов, образующий данный канал: 0,1,2,3,…, l,…, n). Поэтому вполне правомерно использовать и методики и соотношения, полученные в [54,55] Галкиным А.П.

Полный срыв связи между i – ми и всеми j – ми абонентами наступит, если пройдет срыв у всех N абонентов. Вероятность такого события:

$$P_{\sum} = \alpha^N 1^{-\alpha N} = \alpha^N / [\sum_{k=0}^{N} (\alpha^N / N!)]^N$$

Полагая N достаточно большим (N>10 и α<<1), получаем:

$$P_{\sum_{ij}} = \alpha^N / [\sum_{k=0}^{1} (\alpha^k / k!)]^N$$

$y = 1 - \Delta t_{\sum}/t_{\sum} \approx 1 - P_{\sum} = 1 - \alpha^N 1^{-\alpha N}$ и

y^k_{ij}, $y_{\sum ij}$и $y_{\sum i}$, получаем соотношения:

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

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

$y = 1 - \alpha^N 1^{-\alpha N} = 1 - \alpha^N/(1 + \alpha)^N$;

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

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

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

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

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

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

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

Значениям *y* можно придавать смысл уровня проникновений в сети СДО [55, 99-105] и использовать при выборе вариантов проектирования или оценке качества работы сети. Эти расчеты проверялись нами при внедрении в ТГУ и показали удобство оценки и хорошую применяемость в СДО (см. приложения).

3. 4. Оценка эффективности информационного канала СДО с учетом защитных мероприятий

Чаще всего в случае применения защитных мероприятий (ЗМ) в канале дают выигрыш за счет уменьшения расходов на эксплуатационные потери, при этом, $П_{изн} > П_{изс}$ по причине повышения качества.

Тогда приведенные затраты получаются из соотношения [5,54,55, 87,89]

$$П э = \varepsilon + E (Пиз + Км + \ldots) . \qquad (3.4.1)$$

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

$$К_{гку} > К_г \quad при \quad C_{ЗМ} = C \qquad (3.4.2)$$

или

$$К_{гку} = К_г \quad при\ C_{ЗМ} < C \quad , \qquad (3.4.3)$$

Приведем гистограммное выражение сравнений рассчитанное с использованием этой методики для различных алгоритмов (рис.3.4.1-3).

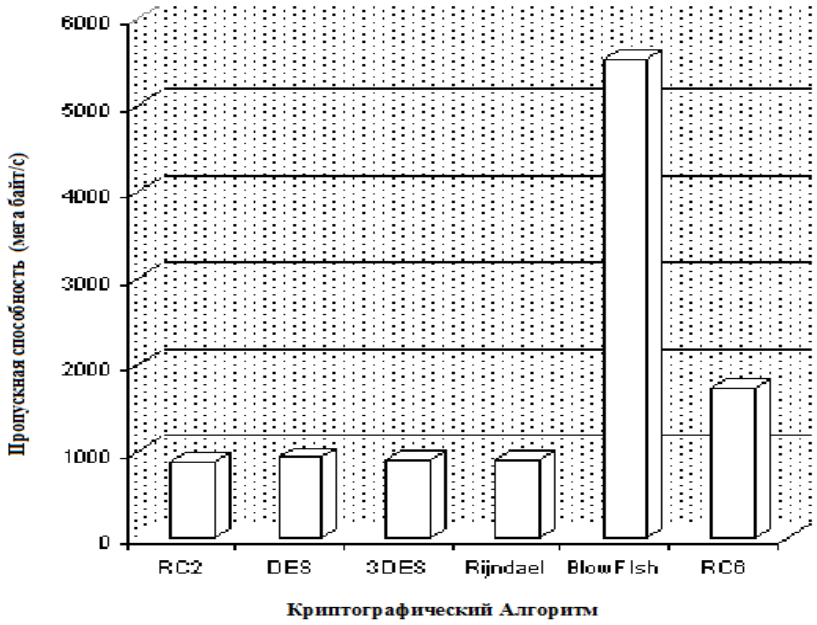


Рис.3.4.1. Пропускная способность каждого алгоритма шифрования (кб /с)

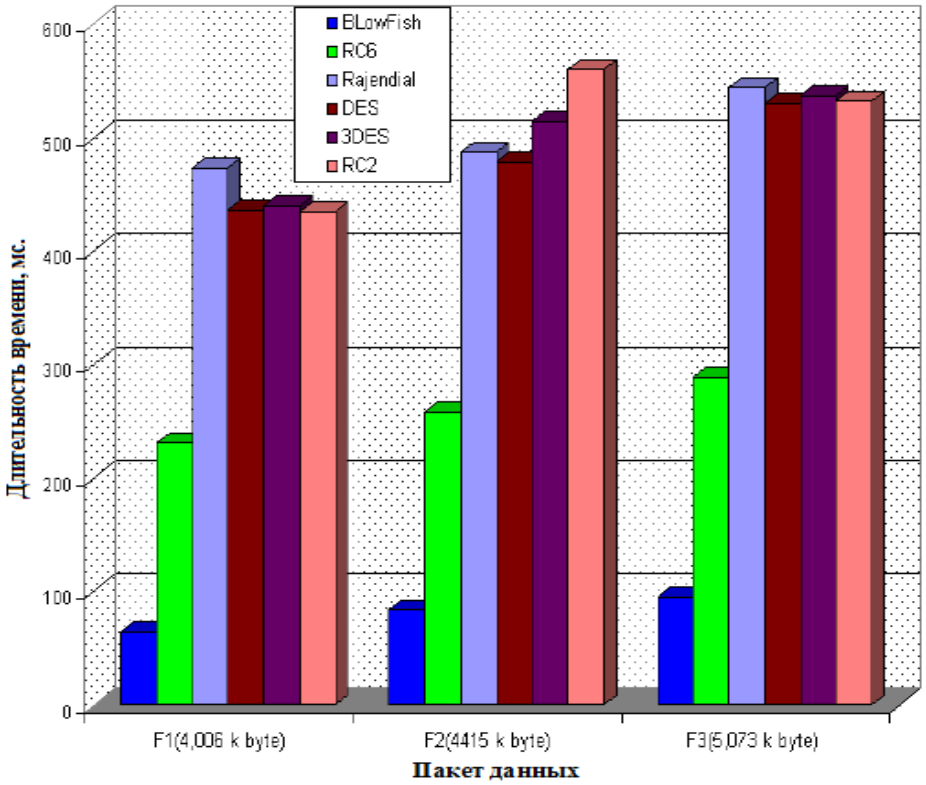


Рис.3.4.2. Время шифрования

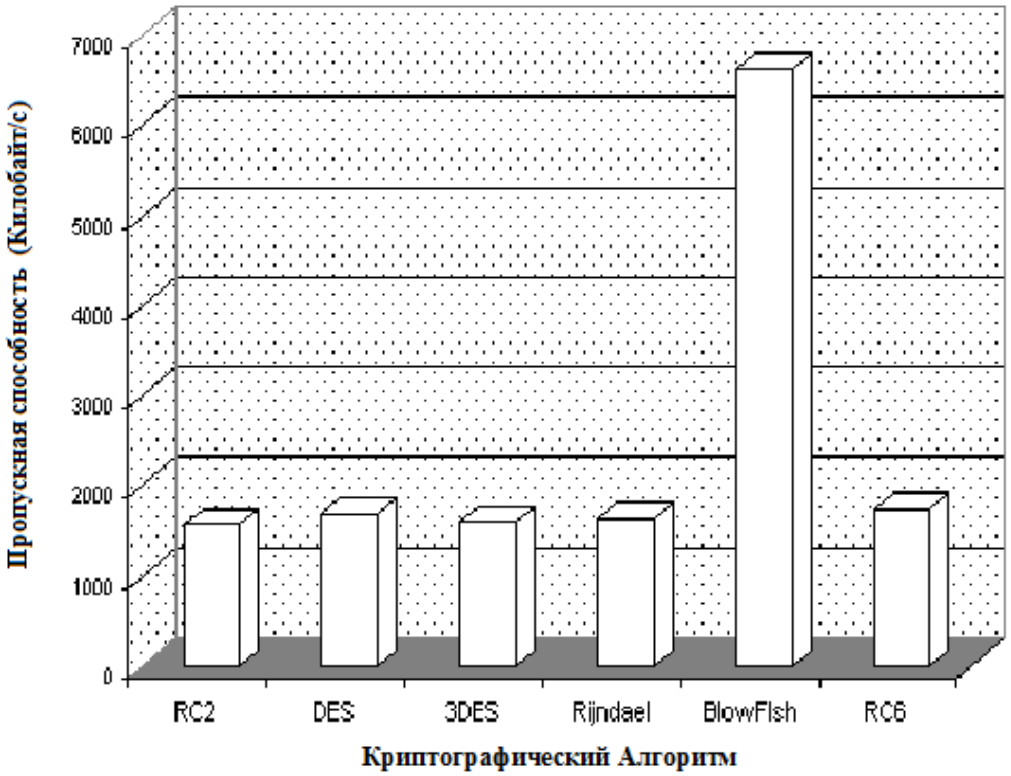


Рис.3.4.3. Скорость каждого алгоритма дешифрования(кб/с)

Достаточную точность позволяют получить эти соотношения при определении эффективности. Для оценки значений составляющих это

соотношение, при отсутствии необходимых данных, можно использовать приближённые математические модели. Кстати, и $С_к$ можно заменить $П_{из}$ и $К_м$. Используя приведённые выше соотношения и методики, приведенные в [54], связывающие характеристики надёжности СДО со стоимостью, можно попытаться найти такие характеристики надёжности, с которыми СДО за определённое время эксплуатации будет иметь наименьшую общую стоимость.

Приводим полученные нами результаты при внедрении в СДО ТГУ (см. приложения).

Практический пример 1: Файлы с различными типами данных.

Это конкретное исследование предпринятых с целью проверки, имеет ли шифрование зависимость от типа данных. Различные типы файлов данных, таких как аудио, изображения, текстовые и видео почти 50 Мб в размере выбраны и время шифрования различных алгоритмов шифрования рассчитывается для этих типов данных (характерных для СДО). Для всех случае у конкретного алгоритма шифрования, варьируя параметр имеем тип данных и постоянные параметры являются ключевыми размер и режим блочного шифра.

Размер ключа и блочного режима находятся в выдерживают при голыми минимальными параметрами. Размер ключа AES, DES, 3-DES, RC2, Blowfish, Skipjack и RC4 хранятся на минимальных значениях, как 128, 56, 112, 40, 32, 80 и 40 бит соответственно. Блочный шифр использующий режим является ECB с PKCS # 5. Рис.3.4.4 показывает время выполнения алгоритмов для разные файлов.

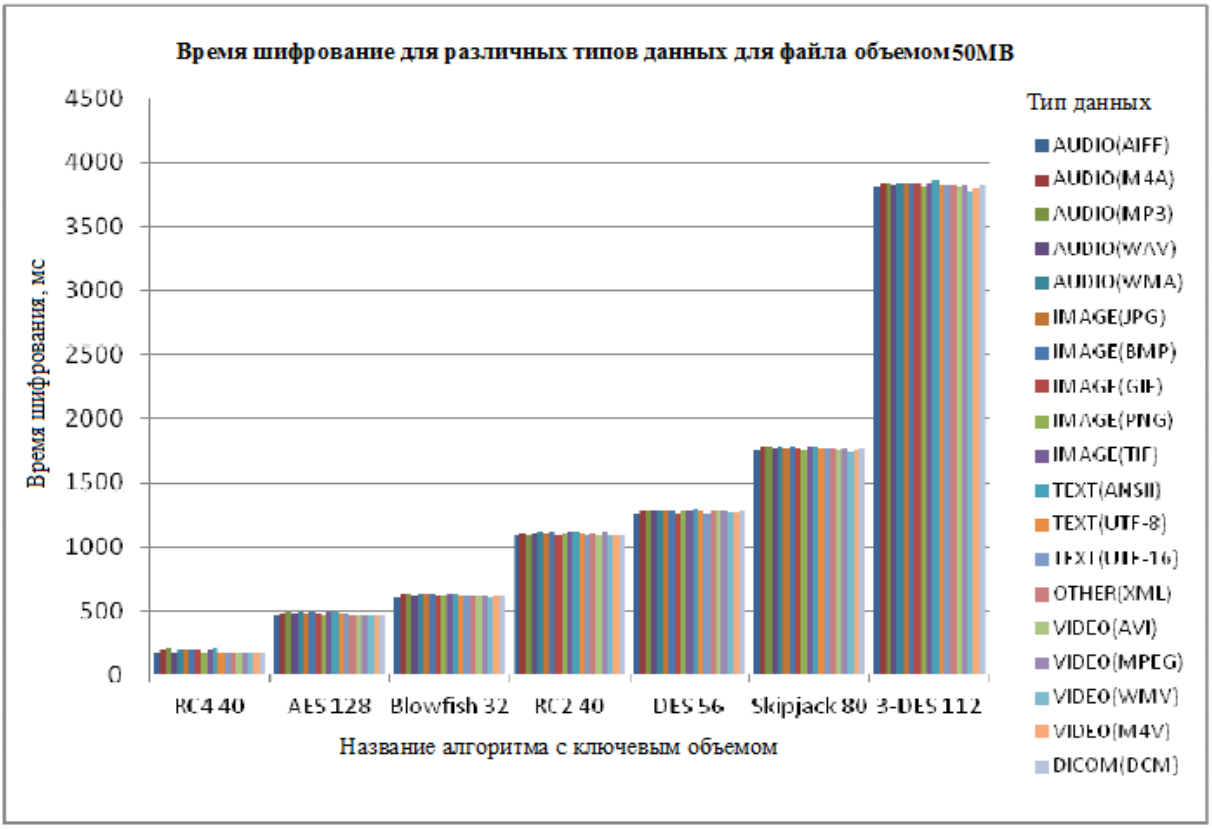


Рис.3.4.4. Время шифрования Vs алгоритм шифрования для файлов различных типов данных

Наблюдение: На рис.3.4.4 можно ясно видеть, что время шифрования для всех типов данных является почти одинаковым. Результат показывает, что время шифрования не меняется в зависимости от типа данных. Шифрование зависит только от числа байтов в файле, а не от типа файла.

Время шифрования AES ниже по сравнению с другими из блочных шифров. RC4 с ключом размером 40 является самым быстрым среди алгоритмов шифрования при испытаниях.

Практический пример 2: Передача файлов с данными того же типа с различными размерами.

Данный случай, принятые для обеспечения вновь наблюдений, полученные в случае исследования 1. Пример 1 показал, что время шифрования зависит от количества байтов в файле. Чтобы обеспечить это еще одно исследование, в котором различные файлы (BMP и FLV) из тех же типов, но разных размеров приведены для шифрования и рассчитывается их время шифрования. Для

всех случаев размер ключа и блочного режима хранятся в минимальных параметрах. В табл.3.4.1 приведены сведения о файлах, используемых для всех случаев и рис.3.4.5-6 показаны результаты выполнения BMP и FLV форматов файлов разных размеров, соответственно.

Таблица 3.4.1. Параметры выполнения для файлов разного размера.

Тип файла	Варьируя параметры (размер данных)	Постоянные параметры
BMP	10.7Мб, 50Мб, 100Мб	Тип данных, Размер ключа
FLV	50Мб, 100Мб, 482Мб	

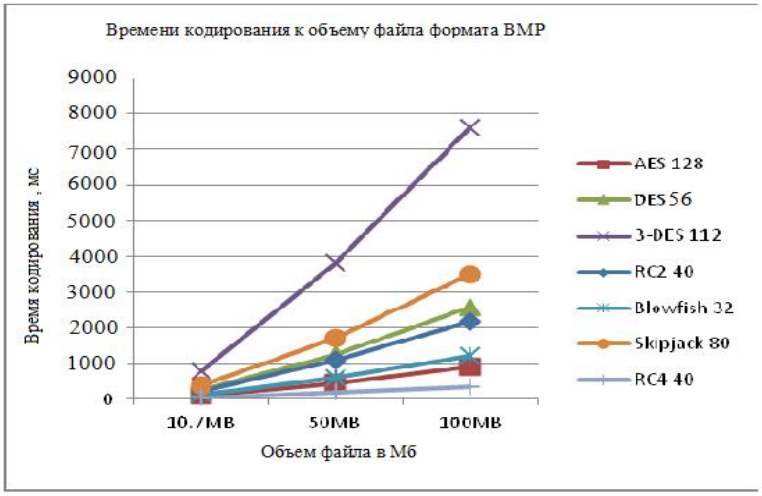


Рис.3.4.5. Размер файла в зависимости от времени шифрования для BMP-файла различных размеров.

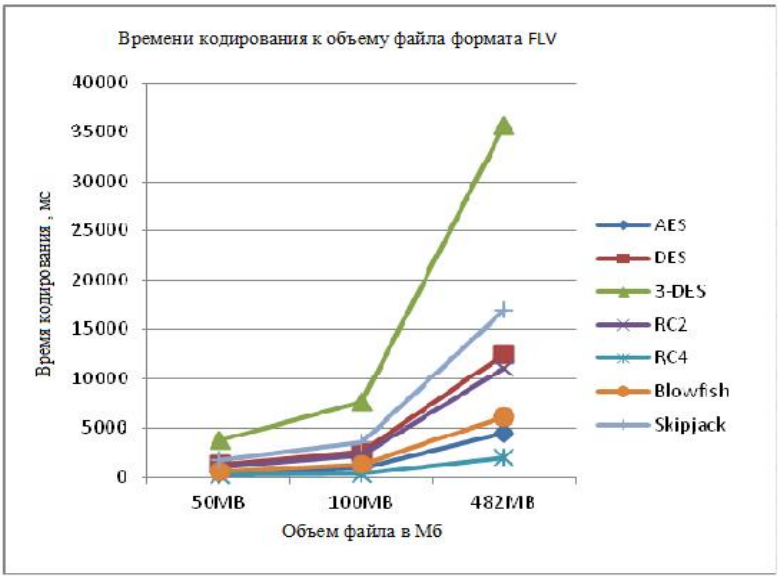


Рис.3.4.6. Размер файла в зависимости от времени шифрования для FLV-файла различных размеров.

Таблица 3.4.2. Время шифрование файлов различных размеров

Тип файла	Размер (в мб)	Время шифрования (миллисекунды)						
		AES	DES	3DES	RC2	BlowFish	Shipjack	RC4
		128	56	112	40	32	80	40
BMP	10.7	101	272	788	238	133	381	40
	50	455	1253	3804	1095	614	1729	198
	100	909	2595	7628	2189	1223	3505	372
FLV	50	456	1268	3810	1112	629	1731	196
	100	918	2586	7631	2224	1267	3515	360
	482	4518	12529	35654	11038	6087	16941	1972

Наблюдение: Для каждого алгоритма шифрования же параметры используются для файлов различных размеров. Табл.3.4.2 показывает время шифрования различных размеров файлов одного типа. Из результатов в табл.3.4.2 и на рис.3.4.5-6, можно найти, что результат для различных размеров данных изменяется пропорционально размеру файла данных. Время шифрования возрастает по мере увеличения размера файлов в кратные размеру данных.

Практический пример 3: Файл с различной плотностью данных.

Это исследование делалось, чтобы проверить, зависит ли шифрование по плотности данных или нет. Скорость шифрования оценивается файла плотности двух различных данных; разреженный файл из 69Mb и плотная файл 58.5Mb. Для алгоритма шифрования, размер ключа и блочного режима хранятся в минимальных параметров. Результаты выполнения приведены в табл.3.4.3.

Таблица 3.4.3. Выполнение для разреженных и плотных данных

Название	Плотный (61392454 байт) AIFF файл	Разреженный (72000118 байт)AIFF файл

алгоритма	Шифрование времени (мс)	Шифрования скорость (Мб/с)	Шифрование времени (мс)	Шифрования скорость (Мб/с)
AES 128	539	108.62	632	108.64
DES 56	1535	38.14	1800	38.14
3-DES112	4363	13.42	5074	13.53
RC2 128	1283	45.63	1518	45.23
BlowFish 128	725	80.75	852	80.59
Shipjack 128	2040	28.70	2384	28.80
RC4 128	216	271.05	251	271.56

Замечание :

Была рассчитана скорость шифрования для разреженных и плотных файлов. Табл.3.4.3 показывает, что время шифрования не зависит от плотности данных в файле. Изменение во времени по отношению к различным алгоритмам по той же схеме для обоих разреженных и плотных файлов. Скорость шифрования для конкретного алгоритма шифрования остается такой же, даже если файл является разреженным или плотным. Это зависит только от количества байтов в файле.

Практический пример 4: Алгоритмы шифрования с различными ключевыми размеров

Это исследование является анализом влияния изменения размера ключа шифрования на время шифрования. BMP файл 50.5мб берется и различные алгоритмы шифрования выполнены для различного размера клавиш, которые с ними в режиме ECB с PKCS # 5.

Различные размеры ключа, указанные в табл.3.4.1, используются во время экспериментов. Рис.3.4.7 показывает результат выполнения для изменения размера ключа.

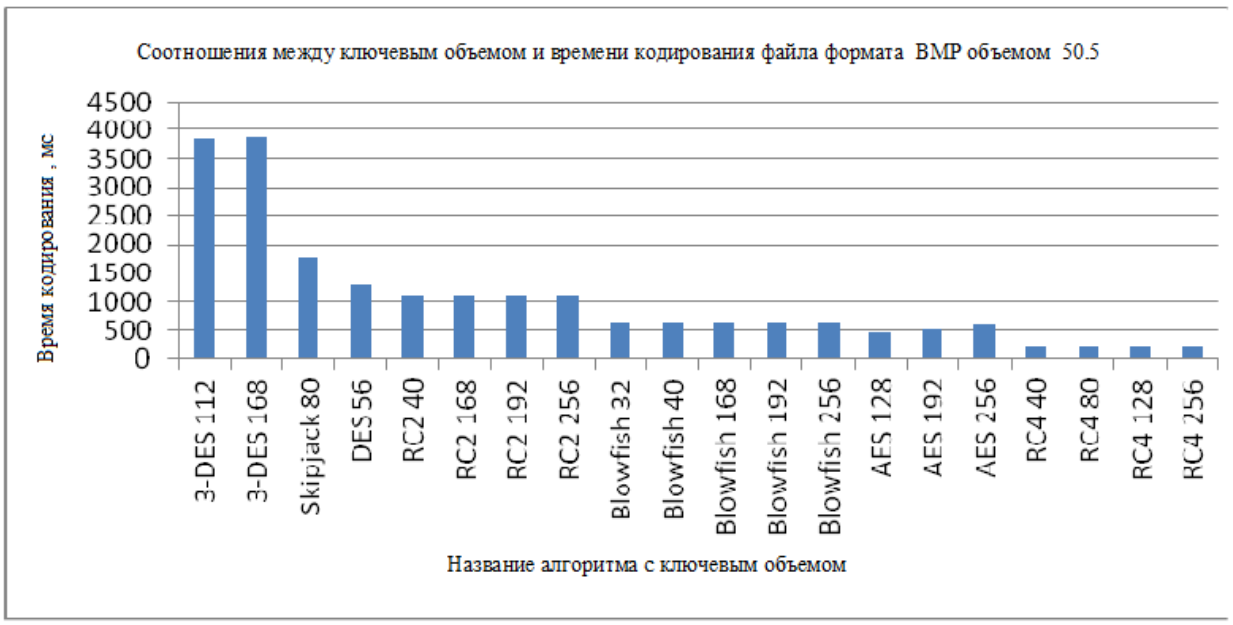


Рис.3.4.7. Изменение размеров ключей для разных алгоритмов шифрования

Замечание:

Результаты показывают, что при выполнении всех алгоритмов, время шифрования изменяется с изменением размера ключа.

Время шифрования возрастает с увеличением размера ключа для блочных шифров. Изменение во времени очень мало. AES доминирует в блочном шифре. RC4 является самым быстрым среди всех алгоритмов испытания.

Выводы. Симметричный алгоритм ключа был проанализирован на различных функциях, таких как файла другого типа данных, плотность записи, размер данных и размер ключа, и анализировалось изменение времени шифрования для различных выбранных алгоритмов шифрования. Из результатов моделирования можно сделать вывод, что время шифрования не зависит от типа данных и плотности файла.

Шифрование зависит только от количества байтов, присутствующих в файле.

Кроме того, установлено, что время шифрования и размер данных пропорциональны друг другу.

По мере увеличения размера данных увеличивается время шифрования пропорционально размеру данных, и наоборот.

Для всех блочных шифров алгоритмы, которых анализируются, с увеличением размера ключа, время шифрования также увеличивается, но уменьшается с увеличением размера ключа для потокового шифра, как RC4. AES является, как представляется, быстрый блочный шифр со скоростью шифрования 108мб/с при минимальных параметрах, но RC4 потоковый шифр. Скорость шифрования 270мб/с - самая быстрая среди всех анализируемых нами алгоритмов шифрования.

Выводы по главе 3

1. Разработанные нами методики решают проблемы обоснования мероприятий по защите от несанкционированного доступа для каждой конкретной СДО в зависимости от задач стоящих перед ними в каждом отдельном случае.
2. Смоделирован информационный канал СДО 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.
5. Разработанные в данной диссертации методики и компьютерные программы, проверены в конкретных СДО ТГУ и показали свою жизнеспособность (см. приложения).

Заключение

1. Рассмотрены основные проблемы в СДО в Йемене и известные пути их решения.
2. Обоснована необходимость защиты телекоммуникаций СДО от несанкционированного доступа к информации с учетом особенностей Йемена поскольку известные методики и структуры не обеспечивают необходимое качество и защищенность.
3. Разработаны методики для поиска несанкционированных проникновений в телекоммуникациях СДО и предложена методика повышения достоверности защищенных запоминающих устройств на 70%.
4. Проанализированы основные особенности защиты информации применительно к республике Йемен на примере ТГУ и разработаны подходы для улучшения эффективности защиты СДО при использовании криптографии и при использовании GSM. При этом число проникновений уменьшилось в 5 раз.
5. Разработанные нами методики решают проблемы обоснования мероприятий по защите от несанкционированного доступа для каждой конкретной СДО в зависимости от задач стоящих перед ними в каждом отдельном случае.
6. Показано, что для СДО в конечном итоге важна эффективность сети связи в зависимости от срывов (в том числе и от проникновений в нее).
7. Разработанные нами расчетные методики позволяют обоснованно оценить эффективность с учетом ограничений.
8. Наши методики разработаны и в виде компьютерных программ, проверены в конкретных СДО Йемена (ТГУ) и показали свою жизнеспособность (см. приложения).

Список литературных источников

1. Карасик А.А. Математическая модель электронного конспекта лекций как компонента электронного учебного курса // Телематика-2003: Труды Хвсерос. науч.-метод. конф. СПб., 2003. - С. 334-335.

2. 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.

3. Карасик А.А., Третьяков В.С. Структура электронного учебника. Технология создания и использования // Технологии информационного общества —Интернет и современное общество: Труды Vвсерос. объединенной конф.СПб., 2002.-С. 189-191.

4. Галкин А.П. Информационная безопасность и целесообразные пути ее улучшения/ Palmarium Academic Publishing - Saarbrucken, Deuchland - 2014.75 с.

5. http://bugtraq.ru/library/internals/admintrap.html

6. Карпов Е.Б., ФридландА.Я.,Фридланд И.А. Учебные материалы для открытого образования // Открытое образование. 2001, № 2. - С. 42-46.

7. 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.

8. 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.

9.Корниенко В.В., Афанасьев А.Н. Модели и средства сетевого обученияXXXIV отчетная науч.-техн. конф. профессорско-преподавательского состава УлГТУ: тез. докл. Ульяновск, 2000.-214 с.

10.Курганская Г.С. Модели, методы и технология дифференцированного обучения на базе Интернет: Автореф. дис. док. физ.-мат. наук. — М., 2001.-32 с.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. Ю.Белкин В.Ю. Разработка образовательных сред на основе полей предметных знаний в системе VEDA. / Белкин В.Ю., Костенко К.И., КурганА.Б., Левицкий Б.Е. // Современная образовательная среда: Материалы всерос. конф. М.: ВВЦ «Наука и образование», 2001 - с. 23-25.

15. 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 Хвсерос. науч.-метод. конф. СПб., 2003.-С.429-431.

16. П.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 Хвсерос. науч.-метод. конф. СПб., 2003. - с. 231-232.

17. 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.

18. 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.

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

20. Деревнина А.Ю, Коняков М.Б., Семекин В.А. Принципы создания электронных учебников // Открытое образование. 2001, № 2. -С. 14-17.

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

22. Ефремов В.С. Виртуальное обучение как зеркало новой информационной технологии. // Менеджмент в России и за рубежом, 1999, № 6.-С.16-18.

23. 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.

24. 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.

25. 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.

26. 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.

27. А.С. № 842766 СССР, Генератор пуассоновского потока импульсов, / Н.М.Ванина, А.П.Галкин и В.В.Орехов, опубл.30.06.81. Бюл. №24.

28. А.С. № 855966 СССР, Генератор случайного импульсного потока, / Н.М.Ванина, А.П.Галкин и В.В.Орехов, опубл. 15.08.81. Бюл. №30

29. Галкин А.П., Лапин А.Н., Самойлов А.Г. Моделирование каналов систем связи, М., Связь, 1979, 96 с.

30. Галкин А.П. Оценка эффективности связи на различных уровнях, Материалы НТК «Эффективность и надежность сложных технических систем», М., МДНТП,1985, с.34-36.

31. Галкин А.П. Назначение рациональных погрешностей контролируемых параметров, «Проблемы метрологического обеспечения систем обработки измерительной информации», Материалы 5-ой всесоюзной конф.,М.,1984, с.131-135.

32. 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.

33. 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

34. Галкин А. П. Устранение несанкционированного использования

диктофона./ Материалы 3-ей Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир, 1999, с.61-64.

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

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

37. 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.

38. Matsunaga, K. Koga, M. Ohkawa, An Analog Speech Scrambling System Using the FFT Technique with High-Level Security. // IEEE Journal on Selected Areas in Communications, v. 7, No.4, May 1989, p. 540-547.

39. Del Re E., Fantacci R., Maffucci D. A New Speech Signal Scrambling Method for Secure Communications: Theory, Implementation, and Security Evaluation. // IEEE Journal on Selected Areas in Communications, v.7, No.4, May 1989, p.474-480.

40. Зарубежная радиоэлектроника. 1989, №12. Специальный выпуск, "Защита информации".

41. Российский портал открытого образования: обучение, опыт, организация/ Отв. ред. В.И. Солдаткин. - М.: МГИУ, 2003. - 508 с.

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

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

44. 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.

45. 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.

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

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

48. Христочевский С.А. Базовыеэлементы электронных учебников и мультимедийных энциклопедий // Системы и средства информатики: Вып. 9 / Под ред. И.А. Мизина. - М.: Наука. Физматлит, 1999. с. 202-214.

49. Юрин В.Н. Компьютерные технологии в учебном процессе инженерного образования // Информационные технологии. 1999, №3.- с. 45-46.

50. Aaron Skonnard. Understanding theIIS Architecture. 1999.http://www. microsoft.com/mind/1099/inside/insidel099.asp (26 апреля 2004)

51. Hebenstreit J. Computers in education - The next step. // Education and Computing, v.l, 1995. -p. 37-43.

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

53. Галкин А.П. Радиосистемы для защиты каналов связи от несанкционированного доступа к информации./Уч. пос.- Владимирский государственный университет.- г. Владимир-2003. 104 с.

54. IIS Architecture.MSDN-Library. 2004. http://msdn.microsoft.com/library/default.asp?url=/library/enus/iissdk/iis/iiscorefunctionality.asp (26 апреля 2004).

55. Internet Information Server 4.0: Пер. сангл. - К.: Издательская группа BHV,1998. - 624 с.

56. А.С. № 714638 СССР, Устройство для задержки импульсов, / А.П. Галкин, В.В.Аксенов и Ж.В.Аксенова , опубл. 05.02.80. Бюл.№5.

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

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

59. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 1999.-568с.

60. Основные положения развития взаимоувязанной сети связи Российской Федерации на перспективу до 2005 г. - М.: Информсвязъ, 1997- 12 книг.

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

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

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

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

65. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

66. Акустика. / А.П. Ефимов, А.В. Никонов, М.А. Сапожков, В.И. Шоров; Под ред. М.А. Сапожкова. -М.: Радио и связь,1989. -336с.

67. Кэнг Г.С. Узкополосный телефонный квантизатор с линейным предсказанием //EASCON 74 Record IEEE Electronicsand Aerospace System Convention. - P. 51-58.

68. Гайкович В., Першин А. Безопасность электронных банковских систем.

-М.: Единая Европа, 1994. - 364 с.

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

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

71. Величкин А.И. Передача аналоговых сообщений по цифровым каналам связи. - М.: Радио и связь, \ 983. - 240 с.

72. Шерстюк Ф. Н. Вирусы и антивирусы на компьютере IBMPC.Персональные компьютеры. Вып. 2. М.: ИНФО АРТ. 1991,189 с.

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

74. Халяпин Д. Б., Ярочкин В. И. Основы защиты информации. М.:ИПКИР, 1994,176 с.

75. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкоммиссии России. М.: Военное издательство, 1992. 385 с.

76. Защита от несанкционированного доступа к информации. Термины и определения. Руководящий документ Гостехкоммиссии России. М.: Военное издательство, 1992. 264 с.

77. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Термины и определения. Руководящий документ Гостехкоммиссии России. М.: Военное издательство, 1992. 248 с.

78. Временное положение по организации разработки, изготовлениии эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах

вычислительной техники. М.: Военное издательство, 1992. 354 с.

79. Закон Российской Федерации «О безопасности».

80. Секреты коммерческой безопасности. Агентство коммерческой безопасности. М. ИНФОАРТ, 1993.234 с.

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

82. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: Единая Европа, 1994. - 364 с.

83. Саломаа А. Криптография с открытым ключом: Пер с англ.- М.: Мир, 1996.-318 с.

84. Калинцев Ю.К. Конфиденциальность и защита информации: Учебное пособие по курсу "Радиовещание и электроакустика". -М.: МТУСИ, 1997. - 60 с.

85. Галкин А.П., Аль-Агбари Мохаммед, Идхилех Мохаммед, Падурянова Н.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.

86. 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.

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.Часть 1. Технические каналы утечки информации. Учебное пособие. М.:Гостехкомиссия РФ, 1998-320 с.

89. 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.

90. ГалкинА.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.

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

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

93. 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.

94. 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.

95. ГалкинА.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.

96. Обади Х.М. Выбор рациональной информационной защиты корпоративных сетей с криптографией/ Галкин А.П., Аль-Джабери Р.Х. , Ковалёв М.С., Суслова Е.Г.// Известия института инженерной физики. 2014.№3(33), с. 7-12.

97. Обади Хезам. Выбор рациональной информационной защиты корпоративных сетей для улучшения конкурентоспособности/ Галкин А.П., Аль-Джабери Р.Х., Суслова Е.Г.// Известия ВУЗов/Технология текстильной промышленности. 2014-№ 4(352), с. 135-137.

98. Обади Хезам. Системный уровень проектирования защищённых сетей / Аль-Джабери Р.Х., Галкин А.П., Ковалёв М.С., Амро М.М.// Известия института инженерной физики.2013-№4. С. 10-12.

99. Обади Хезам. Технико- экономическое обоснование беспроводных сетей для инновационного развития регионов / Галкин А.П., Бадван Ахмед //Управление инновационными процессами развития региона/ Материалы международной научн.- практич. конф., г.Владимир, 2012, с.47-51

100. Обади Хезам. Когнитивное радио - важное направление в инновационном развитии здравоохранении / Галкин А.П., Бадван Ахмед, Аль-ДжаберiРамзи// Труды X Межд. научн. конф. «Физика и радиоэлектроника в медицине и экологии»/ г.Владимир- г.Суздаль, 2012 г., книга 2, с. 176-178.

101. Обади Хезам. Достоверность функционирования отказоустойчивого запоминающего устройства при информационной защите с итеративным кодом /Галкин А.П.,Бадван Ахмед, Аль-ДжаберiРамзи// Труды X Межд. научной конференции «Перспективные технологии в средствах передачи информации»/ г.Владимир- г.Суздаль, 2013 г., книга 2, с. 49-52.

102. Обади Хезам. Экономическая безопасность предприятия и инновационные мероприятия по ее укреплению / Галкин А.П., Бадван Ахмед// Инновационное развитие экономики – основа устойчивого развития территориального комплекса /Материалы межрегиональной научн. конф.- Институт экономики АН РФ, г.Владимир- г.Москва,2012,с.176-184.

103. Обади Хезам. Технико- экономическое обоснование сетей для развития регионов республики Йемена / Галкин А.П.,Аль-Джабери Р.Х., Бадван Ахмед// 2-ой российский экономический конгресс г.Суздаль, 2013-18-22.02. С. 109-111.

104. Obadi H.M. Projection Network-on-Chip as a System-on-Chip platform for safe information / Galkin A.P., Al-Gaberi R.H. Amro M.M.// INDIAN SCINCE CRUISER Volume 27 Number 6 November 2013. С. 35-38.

105. Обади Х. Проектирование медицинских защищенных сетей на

системном уровне/ Галкин А.П. , Аль-Джабери Р. Х.(асп.)// ФРЭМЭ2014-г.Владимир 2014.1-3.07. С.152.

106. Обади Хезам М.А. Влияние характеристик дистанционного обучения на конкурентоспособность вуза // V Международная научно-практическая конференция «Актуальные вопросы развития современного общества»/ Юго-Западный государственный университет (г. Курск, Россия), апрель 2015г.

107. Обади Хезам М.А. Дистанционное обучение как фактор повышения конкурентоспособности вузов // «Обеспечение устойчивого развития регионально экономике в условиях инновационный модернизации производства», г. Владимир-2015г.

108. http://www.cso-yemen.org/content.php?lng=arabic&id=296

Приложения

Приложение 1Йемен и его телекоммуникации

Йемен, Йеменская республика, государство на юго-западе Аравийского полуострова. Площадь Йемена 537 тыс. кв. км. Оно граничит на севере с Саудовской Аравией, а на востоке с Оманом. На юге Йемен омывается водами Аравийского моря и Аденского залива, а на западе – Красного моря . Йемену принадлежат острова Камаран, Перим, Сокотера и др. Йеменская республика была образована 22 мая 1990 в результате объединения Йеменской арабской республики (ЙАР, или Северный Йемен) и Народной Демократической Республики Йемен (НДРЙ, или Южный Йемен). Столица Сана.

Природные условия

Около 2/3 территорий Йемена – сильно пересеченная горная страна (Джабель), состоящая из высоких (до 2-3 тыс. м) плато, расчлененных глубокими долинами, и обрывающаяся на Западе и Юге многоступенчатым сильно эродированным уступом.

На территории Йемена находятся величественные горы, прибрежная низменность Тихама, засушливые пустынные плоскогорья, изредка разделенные более плодородными долинами. В стране осутствуют постоянные водотоки. Территория бывшей ЙАР занимает восточную, самую высокую часть Западно-Аравийского нагорья, которая представляет собой приподнятый, сильно расчлененный край Аравийского щита, частично перекрытый древними лавовыми отложениями. Низменность Тихама, шириной от 30 км до 80 км, сложена аллювиальными и щебнистыми отложениями. Равнина упирается в горы, круто поднимающиеся до высоты 2000-3000 м, где расположено обширное холмистое плоскогорье, пересеченное обычно сухими вади и высокими кряжами; здесь находится самая высокая точка страны – гора Эн-Наби-Шаиб (3660 м). Восточный склон Западно-Аравийского нагорья, обращенный к пустыне Руб-эль-Хали, занимающей большую половину южной части Аравийского полуострова,

более пологий, чем склон, обращенный к низменности Тихама, но более крутой, чем северный склон, обращенный к Неджу. Западная оконечность Руб-эль-Хали возвышается на 900-1200 м над уровнем моря.

Низменность Тихама – жаркий, засушливый район с редкой растительностью. Летние температуры здесь достигают 45 С; осадков выпадает от 150 мм до 400 мм в год. В горных долинах, спускающихся террасами к морю, осадки выпадают более регулярно и составляют более 500 мм в год. В высокогорьях выпадает до 1000 мм осадков. Восточная часть региона отличается засушливым климатом. Для плоскогорий в центре страны характерны теплое лето (до 33С) и прохладная сухая зима.

На территории бывшей НДРЙ большая часть ресурсов, в том числе сельскохозяйственные угодья, сосредоточены в районе Адена. Исключение составляет Хадрамаут, регион в восточной части страны, представляющий собой широкую долину – вади, протянувшуюся параллельно берегу и поворачивающую затем на юг, к морю. Прибрежная низменность на юге простирается на 5-65 км в глубину страны. Внутренняя часть региона представляет собой пересеченное плоскогорье, расчлененное долинами вади. Климат прибрежной полосы такой же жаркий, как и в низменности Тихама, но отличается еще большей сухостью. В некоторых восточных районах выпадает не более 50 мм осадков в год. Климат гор и предгорий восточной части Йемена более умеренный, временами в горах отмечаются заморозки.

Население

Население Йемена состоит в основном из арабских племен, исповедающих ислам. Неарабское население включает главным образом выходцев из Индии, Пакистана и Сомали.

По оценке на 2005г., население составляет 21.3 млн. человек.

Телекоммуникации Йемена

Эта часть экономики развивается динамичнее остальных.

Исторически проводной телефонии в стране было мало и поэтому сейчас сектор мобильной связи приобрел решающее значение.

Таблица Инфраструктура сектора связи, тыс.ед.

	2011	2012	2013
Число тел. линий (установленных)			
Число тел. линий (в обслуживании)	685	798	901
Число абонентов в усложненных системах (Super-Йемен)			1,498
Общее число абонентов в усложненных системах	34	81	126
Общее число абонентов	32	75	109
Общее число пользователей сотовых телефонов(Тел-Йемен)	24	6	
Общее число пользователей сотовых телефонов(GSM)	651	837	1,699
Оптоволоконные	1,686	926	711,44
Использование цифровых технологий(ISDN)	436	285	206
Плотность телефонных линий связи (на 100 жителей)	35,1%	4,13%	4,44%

Приложения 2

```
#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];
   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;
               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;
```

Приложения 2.2

```
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;


}
```

Приложения 2.3

```
#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;
```

Приложение 3

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;

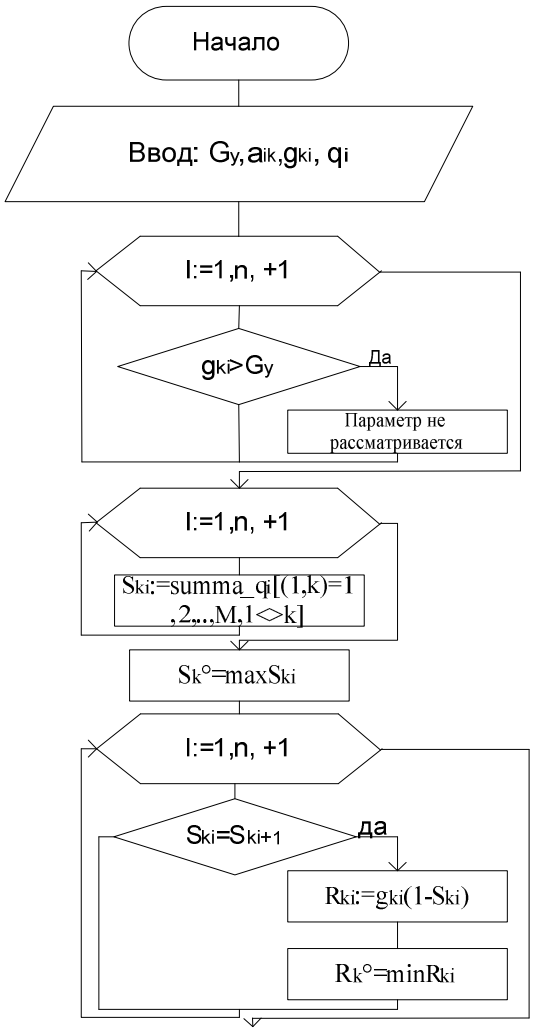
q_i – априорные вероятности отказа i-того элемента;

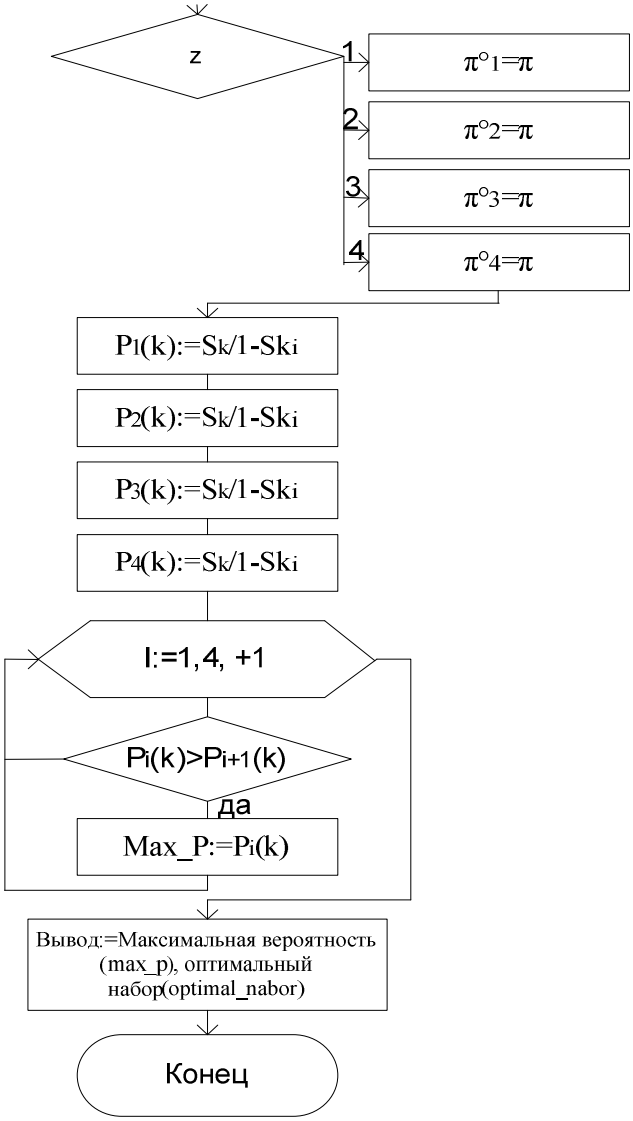
S_k – ненадежность k-го параметра (πk);

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

π_k– параметр;

π°_k– оптимальный параметр;





Выбор контролируемых параметров по максимальным значениям.

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

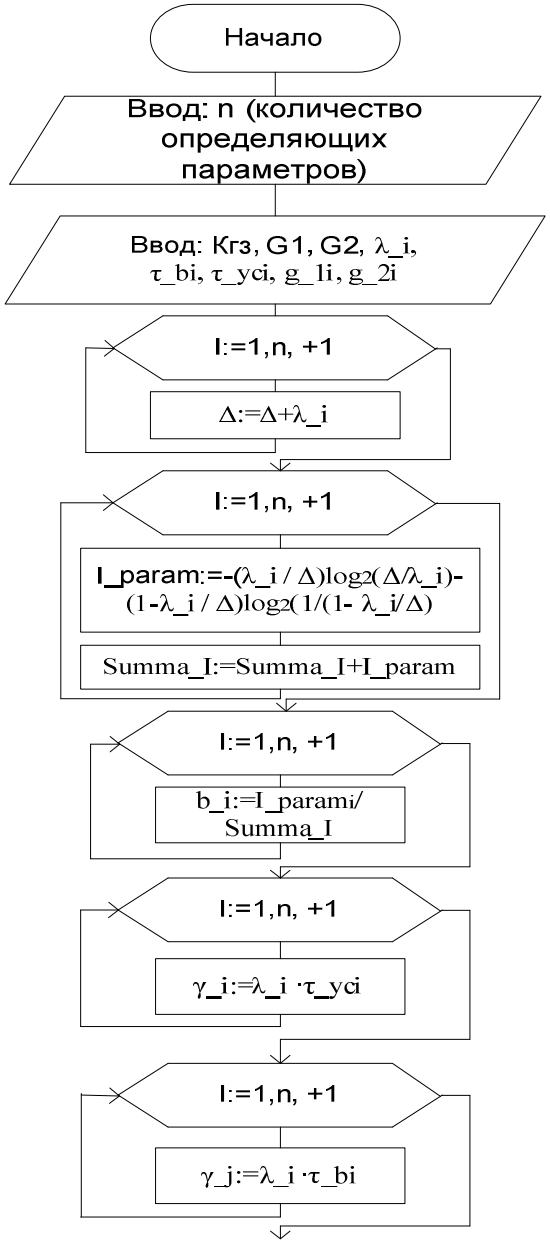
$g_{1,2}$ – достигнутое значение по s-му ограничению;

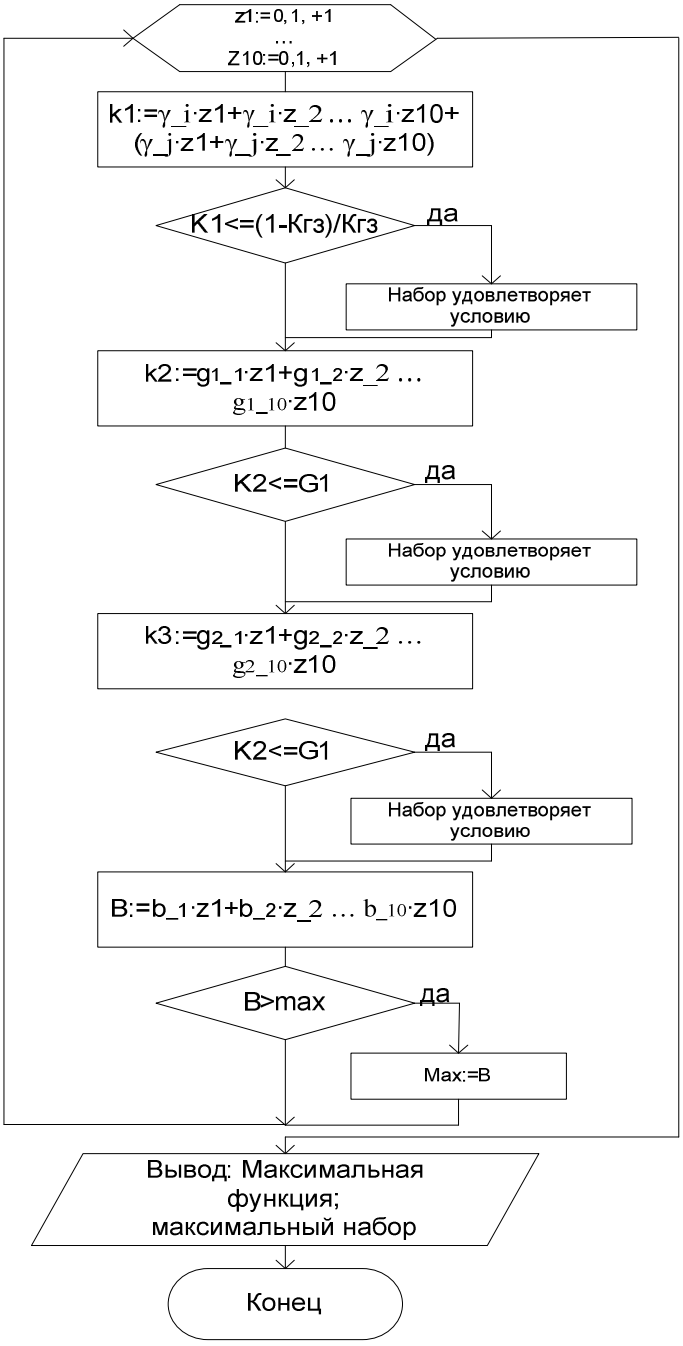
λ_i – интенсивность проникновений в i-тый параметр;

Δ– интенсивность проникновений в канал;

τ_{bi} – время восстановления i-го элемента;

τ_{yci} – время устранения неисправности i-го элемента;


Начало
Ввод: n (количество определяющих параметров)
Ввод: Кгз, G1, G2, λ_i, τ_bi, τ_yci, g_1i, g_2i
I:=1,n, +1
Δ:=Δ+λ_i
I:=1,n, +1
I_param:=-(λ_i / Δ)log2(Δ/λ_i)-(1-λ_i / Δ)log2(1/(1- λ_i/Δ)
Summa_I:=Summa_I+I_param
I:=1,n, +1
b_i:=I_paramі/ Summa_I
I:=1,n, +1
γ_i:=λ_i ·τ_yci
I:=1,n, +1
γ_j:=λ_i ·τ_bi


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

بسم الله الرحمن الرحيم

The republic of Yemen
Taiz University – turba branch
Faculty of Computer Seience
and information technology

الجمهورية اليمنية
جامعة تعز – فرع التربة
كلية الحاسبات وتقنية المعلومات

Date : 15-10-2012

The certificate of introduction

Results received from Mr.Ali Mohamed Hizam Obadi performance of dissertational work are introduced at our University enterprises in the form of settlement techniques and of economic feasibility of improve protection of the information efficiently computer networks . Check of presence of possible methods of penetration in a information systems of our University enterprises .

Recommendation of improve safe for computer networks are used .

Chairman Department
Dr. Mohamed Ibrahim
Al-aghbari

Dean Faculty
Dr. Abdulkarim Shamsan
Aluosofi

Email: doc_mohebrahim2012@yahoo.com

Республика Йемен
Университет Таиз – Филиал Турба
Факультет информатики и информационных технологий
Дата: 15-10-2012

Акт внедрения

Результаты, полученные г-ном. Обади Хезам Мохаммед Али при выполнении диссертационной работы внедрены в нашем университете в виде расчётных методик с расчётом экономической целесообразности улучшения защиты информации компьютерных сетей. Проведена проверка на наличие возможных методов проникновения в системы связи нашего университета, использованы рекомендации по улучшению защиты компьютерных сетей.

Заведующий кафедрой:
к.т.н. Аль-Агбари Мохаммед Ибрагим
Подпись
Печать :(кафедра информатики)
e-mail: doc_mohebrahim2012@yahoo.com

декан факультета:
к.т.н. Аль-Юсофи Абдулкарим Шамсан
подпись
печать: (Университет Таиз)

Перевод с английского языка на русский язык сделан переводчиком:
Аль-Хайдри Валид Ахмед

Город Владимир, Владимирская область, Российская Федерация.
Двадцать шестого ноября две тысячи четырнадцатого года.

Я, Васильева Юлия Николаевна, временно исполняющий обязанности нотариуса нотариального округа города Владимир Селезневой Жанны Игоревны, свидетельствую подлинность подписи, сделанной переводчиком Аль-Хайдри Валид Ахмед Ахмед в моем присутствии. Личность его установлена.

Зарегистрировано в реестре за № **10-7546**.

Взыскано по тарифу: 300 руб. 00 коп.
В том числе взыскано за услуги правового
и технического характера: 200 руб. 00 коп.

Временно исполняющий обязанности

нотариуса нотариального округа

города Владимир Селезневой Ж. И. Васильева Ю. Н.

Прошито, пронумеровано и скреплено печатью на 2 (двух) листах

Временно исполняющий обязанности

нотариуса нотариального округа

города Владимир Селезневой Ж. И. Васильева Ю. Н.