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

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Владимир-2015 г.

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

Научный руководитель **Галкин Александр Павлович**
доктор технических наук, профессор,
кафедры радиотехники и радиосистем
«Владимирский государственный
университет» ВлГУ, г. Владимир.

Официальные оппоненты: **Ромашкова Оксана Николаевна**
доктор технических наук, профессор,
заведующая кафедрой «Прикладная
информатика», «Московский
государственный педагогический
университет» (МГПУ), г. Москва

Кучин Сергей Игоревич
кандидат технических наук,
зам. главного инженера по новой
технике ЗАО «Конструкторское
Опытное Бюро Радио Аппаратуры»,
г. Владимир.

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

Защита состоится « 22 » сентября 2015 г. в 14 ч. в ауд. 301-3 на заседании диссертационного совета Д 212.025.04 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, д. 87, корп. 3, ауд. 301.

С диссертацией можно ознакомиться в научной библиотеке ВлГУ.

Автореферат разослан « 10 » июня 2015 г.

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

Ученый секретарь диссертационного совета
доктор технических наук, профессор  А. Г. Самойлов

Общая характеристика работы

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). 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.

Большую популярность современные виды телекоммуникаций для СДО приобрели в странах, в которых:

- имеются неплотно заселенные территории;
- невысокий жизненный уровень и неустойчивое политическое и экономическое положения;
- Сосредоточение науки и образовательной элиты в нескольких крупных центрах;
- большой уровень неудовлетворенного спроса на СДО и на телекоммуникационные услуги.

Все это полностью относится к Йемену.

Понятно, что на этапах использования защитных технологий в компьютерных телекоммуникациях СДО, возникают трудности, среди кот рых:

-недостаточный компьютерный парк учебных учреждений и индивидуальных пользователей (тьюторов и студентов);

-слабое развитие компьютерных телекоммуникационных сетей СДО, а иногда и устаревшее оборудование;

-недостаточная компьютерная грамотность и информационная культура населения.

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, 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 тематике СДО для Йемена была диссертация Аль - Агбари Мохаммеда, 7 лет назад. С тех пор изменилась технологическая база в стране, изменились ВУЗы. Мы рассматриваем эти проблемы уже с современных позиций. В то же время мы должны 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.

Предметом исследования является разработка методик и алгоритмов обеспечения защиты информации от несанкционированного доступа в СДО Йемена.

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 конкурентоспо-

собности. Для достижения указанной цели в диссертации сформулированы и решены следующие **научные и технические задачи**:

1. Анализ существующих программных продуктов, выполняющих функции защищенных информационных сред для СДО.

2. Оценка требований к структуре СДО и функциональным возможностям отдельных ее компонентов.

3. Разработать принципы и методики поиска технических устройств несанкционированного доступа к информации, которые могут быть реализованы при ограниченных возможностях СДО учебных заведений Йемена.

4. Разработать методику криптографической защиты СДО от несанкционированного доступа.

5. Оценить эффективность информационного канала СДО с учетом защитных мероприятий и показатели надежности, и уровень технического состояния защищаемого канала СДО.

6. Разработать 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 (ТГУ).

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 значимость - 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.

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, 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.; 10,11-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-Суздаль- г. Москва,2013.

Публикации. Основное содержание работы изложено в 11-ти статьях и трудах НТК (из них 3 из списка ВАК), в отчетах Госбюджетных НИР кафедры радиотехники и радиосистем №118 (2012-2014г.). На международных научно-технических конференциях и семинарах сделано 5 докладов и сообщений.

Личный вклад автора диссертации. В диссертации использованы результаты исследований и разработок по созданию многофункциональных мето-

дик и аппаратных средств для защиты систем связи и корпоративных сетей от несанкционированного доступа к информации. При этом автор диссертации являлся непосредственным исполнителем или соавтором основополагающих разработок, алгоритмов и моделей. В статьях и в докладах, выполненных в соавторстве, ему принадлежит или равная часть или более того.

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

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность работы, сформулированы цели и задача исследований с учетом особенностей СДО Йемена, научная новизна, приводятся положения выносимые на защиту и практическая значимость результатов диссертации.

В первой главе диссертации представлен краткий обзор научной литературы по тематике диссертации и особенностей Йемена. Рассматривается несанкционированный доступ к информации в корпоративных сетях СДО, анализ технических каналов корпоративных сетей по несанкционированному доступу и защите от него, финансовая устойчивость и информационная безопасность образовательного учреждения.

Даны классификация и характеристика технических каналов утечки информации, обрабатываемой техническими средствами. Рассмотрены защита телекоммуникаций образовательных учреждений с особенностями, свойственными для Йемена, информационные сети Йемена, анализ технических каналов корпоративных сетей по несанкционированному доступу и защите от него, технологическая устойчивость, конкурентная способность и информационная безопасность предприятия, универсальные угрозы для корпоративных систем, атаки типа отказ в обслуживании в СДО, особенности информационной безопасности государственных сетей Йемена, оценка эффективности информационного канала с учётом защитных мероприятий.

Во второй главе показано, что 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). 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. Поэтому произведем оценку выигрыша приближенным способом. Вводится величина $P_{\text{п}}$ – вероятность ПИП при защите из-за ошибок обслуживающего персонала, равная.

$$P_{\text{п}} = P_{\text{по}} + P_{\text{пу}},$$

где $P_{\text{по}}$ и $P_{\text{пу}}$ – вероятности повреждения канала при отыскании и устранении проникновений соответственно.

Находим коэффициент повторных неисправностей $К_{\text{пн}}$ по формуле

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

Поэтому при автоматических мероприятиях по защите канала (АМЗК) СДО в предположении того, что при отказах элементов любых типов величина $P_{\text{п}} = \text{const}$, при АМЗК

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

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

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

В этом случае легко можно найти выигрыш во времени восстановления канала СДО по формуле

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

Эту методику мы применили для расчетов при внедрении защитных мероприятий в ТГУ.

При проектировании защищенных СДО Йемена возникают проблемы выбора защиты (и бюджетной и эффективной). Обоснуем и приведем разработанный нами подход, удовлетворяющий этим условиям. Предварительно проведем целевую классификацию для таких сетей. Алгоритмы шифрования с использованием ключей предполагают, что данные не сможет прочитать никто, кто не обладает ключом для их расшифровки. *Симметричные алгоритмы.* Для шифрования и расшифровки используются одни и те же алгоритмы. Один и тот же секретный ключ используется для шифрования и расшифровки. Этот тип алгоритмов используется как симметричными, так и асимметричными криптосистемами. *Асимметричные алгоритмы* используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей (которые используются для шифрования самих данных). Используется два разных ключа - один известен всем, а другой держится в тайне. Обычно для шифрования и расшифровки используется оба этих ключа. Но данные, зашифрованные одним ключом, можно расшифровать только с помощью другого ключа.

Приведем разработанный нами подход к защите информационной безопасности СДО при использовании каналов с GSM на примере сети ТГУ (Йемен).

Первоначально в аналоговых системах сотовой связи первого поколения процедура аутентификации имела простейший вид: подвижная станция передавала свой уникальный идентификатор (электронный серийный номер — Electronic Serial Number, ESN), и если таковой отыскивался среди зарегистрированных в домашнем регистре, процедура аутентификации считалась успешно выполненной. Подобная простейшая аутентификация оставляла большие возможности для фрода, поэтому со временем и в аналоговых системах, и тем более в системах сотовой связи второго поколения с использованием дополнительных

возможностей цифровых методов передачи информации, процедура аутентификации была значительно усовершенствована.

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

Процедура аутентификации стандарта GSM в СДО показана на рис.1.

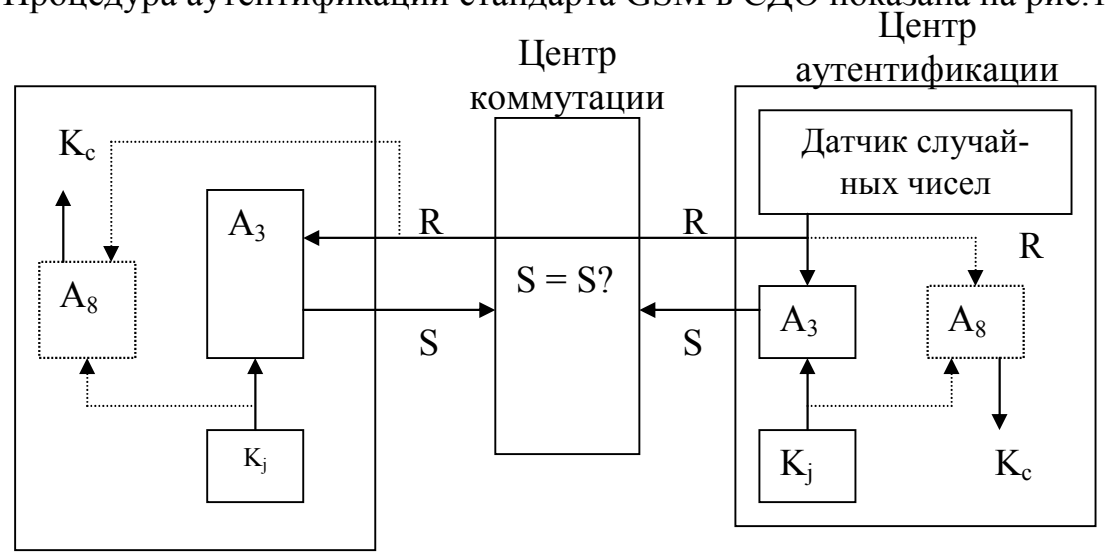

Рис. 1. Схема процедуры аутентификации в стандарте GSM: — случайное число; A3 — алгоритм аутентификации; A8 — алгоритм вычисления ключа шифрования; Ki — ключ аутентификации; Kc — ключ шифрования; S — зашифрованный отклик(Signed Response-SRES).

Работа по обеспечению секретности UMTS 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 представлена архитектура обеспечения секретности в сетях 3G, как определено для версии 4.

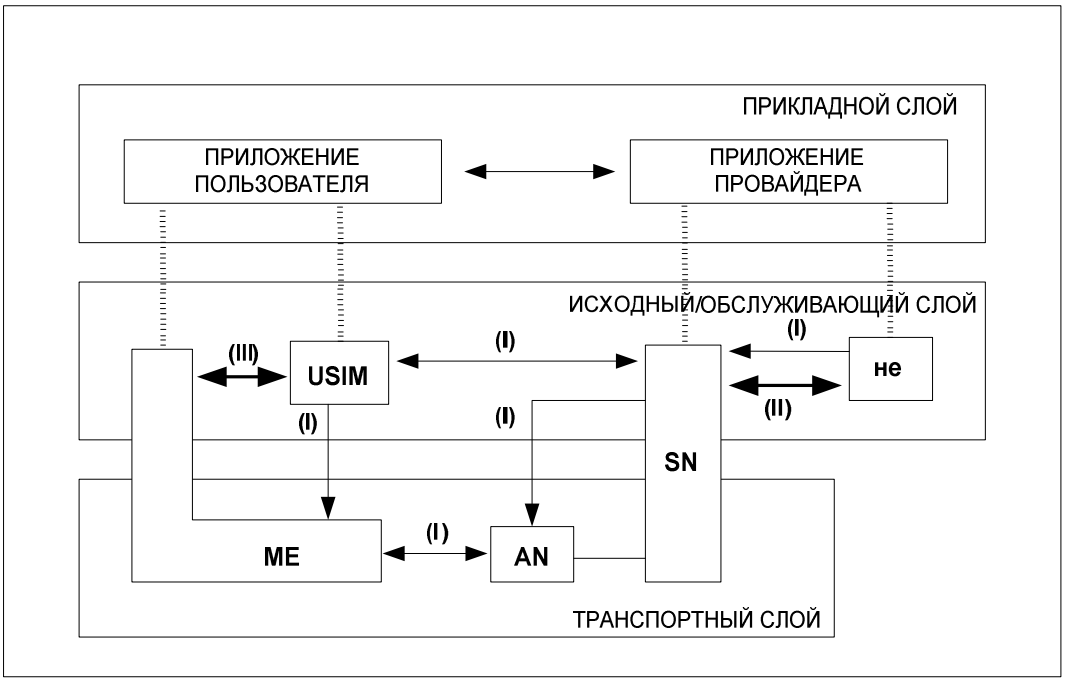

Рис. 2..Обзор архитектуры обеспечения секретности в 4-й версии

В третьей главе рассмотрены оценка целесообразности организации защиты информации от несанкционированного доступа в СДО Йемена, угрозы, проникновения и защита от них, эффективность защитных мероприятий в СДО.

Для каждого типа угроз может быть одна или несколько мер противодействия. 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.

Эффективность систем связи СДО зависит, в частности, от количества и длительности срывов связи между различными абонентами и центрами. 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 K_l (l – число абонентов, образующий данный канал: 0,1,2,3,…, l,…, n). Допустим,

$$\sum_{l=0}^{n} K_l = n_{ji}$$

что в образовании каналов связи задействованы все абоненты сети таким образом, что каждый из них участвует только в одном канале.

- полное число каналов связи между i – м и j – м абонентами;

$$K_0 + \sum_{l=1}^{n} K_l \, l = N\text{-}1$$

- где n – максимальное число абонентов в канале:

Для такой системы выполняется это равенство.

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

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

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

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

Окончательно для определения зависимостей между:

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

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

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

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

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

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

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

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

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

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

Итоговые соотношения

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

Значениям y можно придавать смысл уровня технического состояния сети СДО (или соответствующей ее части) и использовать при выборе вариантов проектирования или оценке качества работы сети. Эти расчеты проверялись нами при внедрении в СДО ТГУ и показали удобство оценки для них мы разработали и внедрили и алгоритмы и программы.

В наших задачах шифрования при внедрении мы также рассмотрели передачу файлов с различными размерами. При этом 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.1 приведены сведения о файлах, используемых для всех случаев, а на рис.3-4 показаны результаты выполнения BMP и FLV форматов файлов разных размеров, соответственно.

Таблица 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	

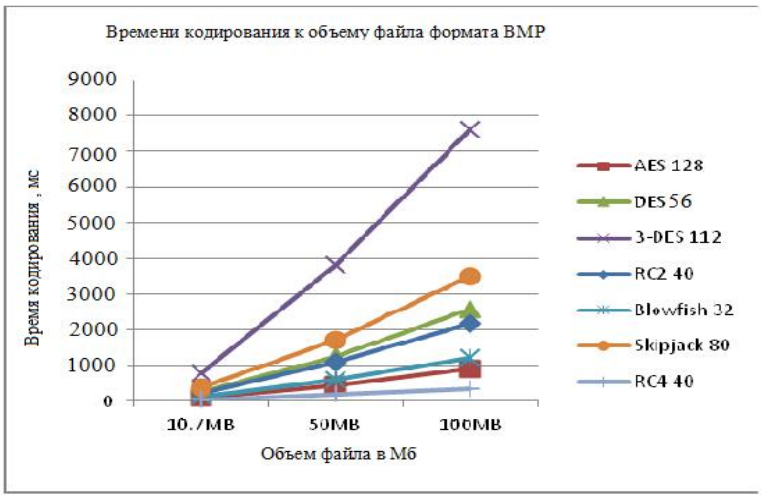

Рис.3. Размер файла в зависимости от времени шифрования для BMP-файла различных размеров.

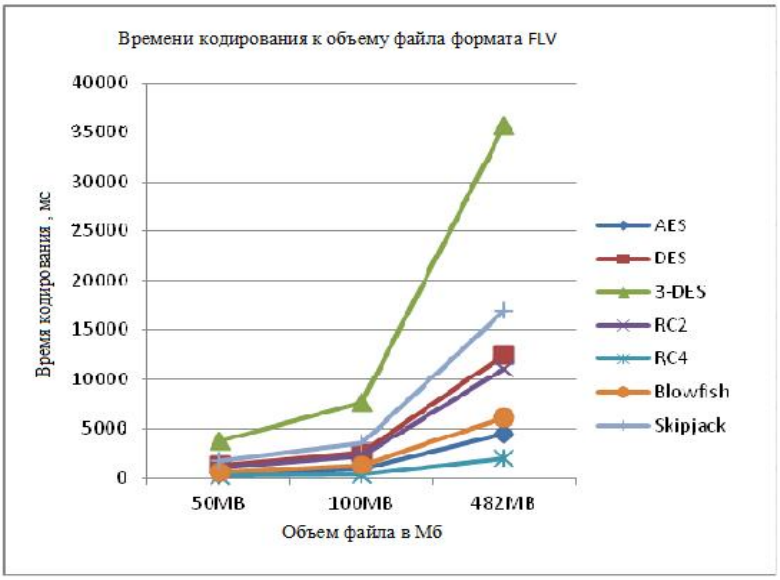

Рис.4. Размер файла в зависимости от времени шифрования для FLV-файла различных размеров.

Таблица 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.2 показывает время шифрования различных размеров файлов одного типа. Из результатов в табл.2 и на рис.3-4, 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.

Основные результаты диссертационной работы:

В ходе проведенных исследований получены следующие основные результаты:

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.

Список публикаций по теме диссертации

- в изданиях по перечню ВАК:

1. Обади Хезам. Системный уровень проектирования защищенных сетей / Аль-Джабери Р.Х., Галкин А.П., Ковалёв М.С., Амро М.М.// Известия института инженерной физики.2013. №4. - С. 10-12.(30%).

2. 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.(30%).

3. 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. (35%).

- в других изданиях:

4. Обади Хезам. Когнитивное радио-важное направление в инновационном развитии здравоохранении / Галкин А.П., Бадван Ахмед, Аль-Джабери., Рамзи // Труды X Международной научной конференции «Физика и радиоэлектроника в медицине и экологии».Владимир-Суздаль, 2012 г., книга 2. С. 176-178. (35%).

5. Обади Хезам. Техника- 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. (35%).

6. 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 АН РФ, Владимир-Москва, 2012. С.176-184. (35%).

7. Обади Хезам. Достоверность функционирования отказоустойчивого запоминающего устройства при информационной защите с итеративным кодом /Галкин А.П., Бадван Ахмед, Аль-Джабери Рамзи // Труды X Международной научной конференции «Перспективные технологии в средствах передачи информации»/ Владимир-Суздаль, 2013 г., книга 2. С. 49-52. (35%).

8. Обади Хезам. Техника- 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. С. 109-111. (35%).

9. 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. (30%).

10. Обади Хезам. Проектирование медицинских защищенных сетей на системном уровне/ Галкин А.П., Обади Х.М.// МНК ФРЭМЭ-2014-Владимир-Суздаль, 1-3.07.2014. Том 2. С.152-154.

11. 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. С. 42-44.

Подписано в печать 01.06.2015.
Формат 60×84/16. Усл. печ. л. 1,39. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.