На правах рукописи

Амро Мохаммад Махмуд Сулейман

ИНФОРМАЦИОННАЯ ЗАЩИТА МЕДИЦИНСКИХ КОМПЬЮТЕРНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В ИОРДАНИИ

Специальность 05.12.13 – Системы, сети и устройства телекоммуникаций

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Владимир 2016

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

Научный руководитель — **Галкин Александр Павлович**
доктор технических наук, профессор
кафедры радиотехники и радиосистем
Владимирского государственного
университета имени Александра
Григорьевича и Николая Григорьевича
Столетовых (ВлГУ), г. Владимир

Официальные оппоненты: — **Приоров Андрей Леонидович**
доктор технических наук, доцент
кафедры «Динамики электронных систем»,
Ярославского государственного
университета имени Демидова

Кучин Сергей Игоревич
кандидат технических наук
ведущий инженер ЗАО «Конструкторское
опытное бюро радиоаппаратуры»,
г. Владимир

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

Защита состоится «28» декабря 2016 г. в 16.00 часов на заседании диссертационного совета Д 212.025.04 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, д. 87, корп. 3, ауд. 301.

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

Автореферат разослан «24»октября 2016 г.

Отзывы в двух экземплярах, заверенные печатью, просим направлять по адресу: 600000, г. Владимир, ул. Горького, д. 87, ВлГУ, ФРЭМТ, секретарю диссертационного совета Д 212.025.04.

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

Актуальность

Всемирные компьютерные сети дали возможность применения информации и интеллектуального багажа практически любого предприятия. Использовать эти возможности для благородных задач медицинских организаций (результаты анализов, статистика, рецепты, запись на прием, документы и т.п.) очевидно самая актуальная и благородная задача для всех телекоммуникаций.

Это объясняется многими причинами, основными среди которых можно назвать приведенные в таблице 1:

Таблица 1

Основные причины и характеристики	Применимость к Иордании
невозможность отрываться от повседневного процесса; необходимость повышать качество медицинских услуг, уменьшать при этом затраты на коммуникации, автоматизацию и управление	полностью
недостаточным уровнем жизни и неустойчивыми политическим и экономическим состояниями	частично
имеющим большой спрос на все виды телекоммуникаций	полностью

Эти факторы в большой степени относятся к Иордании.

Опыт международных исследований и разработок показывает, что во многих странах мира уже ряд лет успешно развиваются технологии, позволяющие использовать Интернет для телекоммуникаций медицинских учреждений (МУ).

Очевидно, что на начальных этапах внедрения в Иордании компьютерных телекоммуникаций в медицинские организации могут возникнуть существенные трудности и помехи, указанные в таблице 2:

Таблица 2

Трудности и помехи	Наличие в Иордании
недостаточно насыщенный компьютерный парк а, часто он еще и устаревший, без возможностей обновления	есть
недостаточное развитие медицинских компьютерных телекоммуникационных сетей (МКТС), их информационная незащищенность	частично
недостаточная компьютерная грамотность и информационная культура и медицинского персонала и населения, что создает дополнительные психологические барьеры в развитии высококачественных МКТС	частично

А ведь при этом главная задача сохранение здоровья людей.

В Иордании представлено достаточно большое число программных продуктов, предназначенных для осуществления информационного и программного обеспечения телекоммуникационных сетей. Однако для МКТС большая их часть не удовлетворяет критериям, предъявляемым к ним с точки зрения защиты информации от несанкционированного доступа.

Другим важным фактором, сказывающимся на сложности непосредственного использования предлагаемого программного обеспечения, является необходимость адаптации функциональных возможностей приобретаемого продукта и его открытость для взлома, внедрения ошибок и потери информации, иногда жизненно важной!

Поэтому разработка информационно-программной среды, учитывающей требования современных иорданских МКТС, а также особенности состояния сетевых коммуникаций регионах, представляется чрезвычайно актуальной в современных условиях.

Объект исследования – системы телекоммуникаций медицинских учреждений в Иордании.

Предмет исследования – методики и алгоритмы для обеспечения защиты информации от несанкционированного доступа в МКТС Иордании**.**

Цель работы – решение научно-технической задачи, связанной с созданием комплекса методик для повышения помехозащищенности связи и разработкой методик и средств по обеспечению информационной безопасности систем связи и оценки их эффективности.

Для достижения указанной цели в диссертации требуется сформулировать и решить следующие **задачи**:

- разработать принципы компоновки архитектуры МКТС и управления их информационными потоками;
- выполнить оценку требований к структуре МКТС и к функциональным возможностям отдельных ее компонентов.
- создать программно-аналитические средства информационного сопровождения и поддержки принятия решений по планированию и сопровождению медицинского центра;
- исследовать эффективность наиболее распространенных методов шифрования информации при их реализации в МКТС Иордании и разработать шифрование для конкретного медицинского центра;
- разработать методику расчёта эффективности мероприятий по защите от несанкционированного доступа и оценить эффективность информационного канала МКТС с учетом защитных мероприятий.

Методы исследования – При решении поставленных задач использован аппарат математического анализа, теории вероятностей и случайных процессов, теории надежности, вычислительной математики и программирования.

Основные теоретические результаты проверены путем расчетов и в ходе испытаний и эксплуатации МКТС и защите их от несанкционированного доступа к информации.

Научная новизна – работы заключается в следующем:

- построена методика расчета сетей и защиты информации в них и проведен синтез пользовательской структуры для информационной защиты МКТС Иордании;

- выработаны принципы компоновки корпоративной информационно-управляющей сети на примере медицинского центра в Аммане;
- предложены принципы планирования организационной структуры информационно-управляющей сети;
- разработаны алгоритмы определения состава комплекса средств защиты информации и эффективности защиты в МКТС для Иордании.

Практическая значимость – работы заключается в следующем:

1. Проверено, что использование разработанного шифрования позволяет улучшить информационную защиту в среднем в 4 раза;
2. Использование предложенного алгоритма по минимизации роутеров позволило уменьшить их число в 2 – 5 раз и сократить время проектирования МКТС в 3 раза;
3. Использование разработанного автором алгоритма по оценке эффективности защиты на этапе расчетов и проектирования МКТС позволило уменьшить время в 3 раза и повысить точность оценки на 70 % при диагностике информационного канала в медицинских сетях.

Основные положения, выносимые на защиту:

1. Обоснование мероприятий по защите от несанкционированного доступа и различных проникновений.
2. Методика определения зависимости эффективности сети связи от срывов.
3. Оценка эффективности информационного канала с учетом защитных мероприятий.
4. Теоретическое определение выигрыша во времени использования канала за счет уменьшения числа ошибок при отыскании проникновений и защите канала.
5. Оптимизация информационной защиты учреждений и предприятий за счет использования итеративных малоразрядных кодов и объединения маршрутизаторов.

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

В диссертации использованы результаты исследований и разработок по созданию многофункциональных методик и аппаратных средств для защиты систем связи и других технических устройств предприятий и учреждений от несанкционированного доступа к информации с оценкой их эффективности по критериям и методикам, предложенных автором.

Результаты внедрения работы. Основные теоретические и практические результаты работы внедрены в виде программных продуктов по защите информации в каналах, алгоритмов и методик шифрования в медицинском центре в Аммане (Иордания). Внедрение результатов исследований подтверждено соответствующими документами.

Апробация работы. Основные научные и практические результаты работы докладывались и обсуждались в 8 докладах и сообщениях на 6-ти международных конференциях: 10-ой и 11-й международной научно технической конференции «Перспективные технологии в средствах передачи информации», г. Владимир, 2013, 2015гг.; X-X11 международной научно-технической конференции «Физика и радиоэлектроника в медицине и экологии» (ФРЭМЭ), г. Владимир, 2012, 2014, 2016гг.; на 2-м международном экономическом конгрессе, г. Владимир - г. Суздаль - г. Москва, 2013г.

Публикации

Основное содержание работы изложено в 12-ти статьях и трудах НТК (из них 3 из списка ВАК, одна в зарубежном журнале), в отчетах Госбюджетных НИР кафедры радиотехники и радиосистем ВлГУ (2012-2016 гг.). На международных научно-технических конференциях и семинарах сделано 8 докладов и сообщений.

Личный вклад автора диссертации. В диссертации использованы результаты исследований медицинских компьютерных телекоммуникационных сетей Иордании и разработок по созданию многофункциональных

методик, в том числе методики криптографической защиты и методики аутентификация согласование ключей 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 объём диссертации.

Диссертация состоит из введения, 4 глав, заключения и библиографического списка, включающего 137 наименований, и 4-х приложений. Объём диссертации: 149 страниц основного текста, 56 рисунков и 59 таблиц.

Основное содержание работы

Во введении обоснована актуальность работы, сформулированы цели и задача исследований с учетом особенностей МКТС Иордании, 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 информационных особенностей Иордании и ее медицинских сетей. Рассматривается несанкционированный доступ к информации в МКТС, анализ технических каналов корпоративных сетей по несанкционированному доступу и защите от него, информационная безопасность МУ.

Даны классификация и характеристика технических каналов утечки информации, обрабатываемой техническими средствами. Рассмотрены защита телекоммуникаций медицинских учреждений с особенностями, свойственными для Иордании, информационные сети Иордании, анализ технических каналов корпоративных сетей по несанкционированному доступу и защите от него, универсальные угрозы для корпоративных систем, особенности информационной безопасности государственных сетей Иордании, оценка эффективности информационного канала с учётом защитных мероприятий.

Таблица 3. Характеристики систем управления базами данных в Иордании.

Характеристика	Informix Dynamic Server	Microsoft SQL Server 2000	Oracle9i Database
Производительность	На небольших объемах практически одинакова		
	Высокая	Средняя	Средняя
Надежность	Высоконадежная	Надежная	Высоконадежная
Масштабируемость	Высокая	Средняя	Высокая
Разграничение доступа	Стандартные средства	Стандартные средства	При наличии специальной версии сервера полный контроль вплоть до конкретной ячейки
Форматы данных	Поддержка всех современных форматов	Поддержка всех современных форматов	Поддержка всех современных форматов
Централизованное администрирование	Есть	Есть	Есть
Планировщик процессов	Есть	Есть	Есть
Операционные системы	Широкий спектр	Только Windows	Широкий спектр
Техническое обеспечение	Средние требования	Средние требования	Средние требования
Уровень поддержки в Иордании	Низкий	Высокий	Высокий
Стоимость	Высокая	Низкая	Высокая

Все каналы связи в Иордании с точки зрения защиты информации и проникновений, близки и отличаются только скоростями и объёмами памяти, мы будем уделять основное внимание МКТС, пока обделенными информационной защитой и в том числе шифрованием. Поэтому наше рассмотрение этих вопросов актуально для Иордании.

Во второй главе проведена оценка достоверности функционирования отказоустойчивых запоминающих устройств (ЗУ) рассмотренная на примере медицинского центра в Аммане с использованием кодирования (шифрования).

Оценку влияния кратности исправляемой ошибки аппаратурные затраты и достоверность функционирования устройств памяти при реализа-

ции кодирования информации при различных кратностях ошибок приводим в работе в виде полученных результатов и зависимостей, отображающих достоверности функционирования запоминающего устройства от времени. Исходя из этого, считаем возможным применять и для шифрования в МКТС Иордании малоразрядных кодов. Для проверки, разработанного нами шифрования, разработали алгоритм и программу и провели эксперимент при внедрении для сетей медицинского центра в Аммане. Блок - схема приведена на рис.1, на рис.2, логика алгоритма, на рис.3, интерфейс.

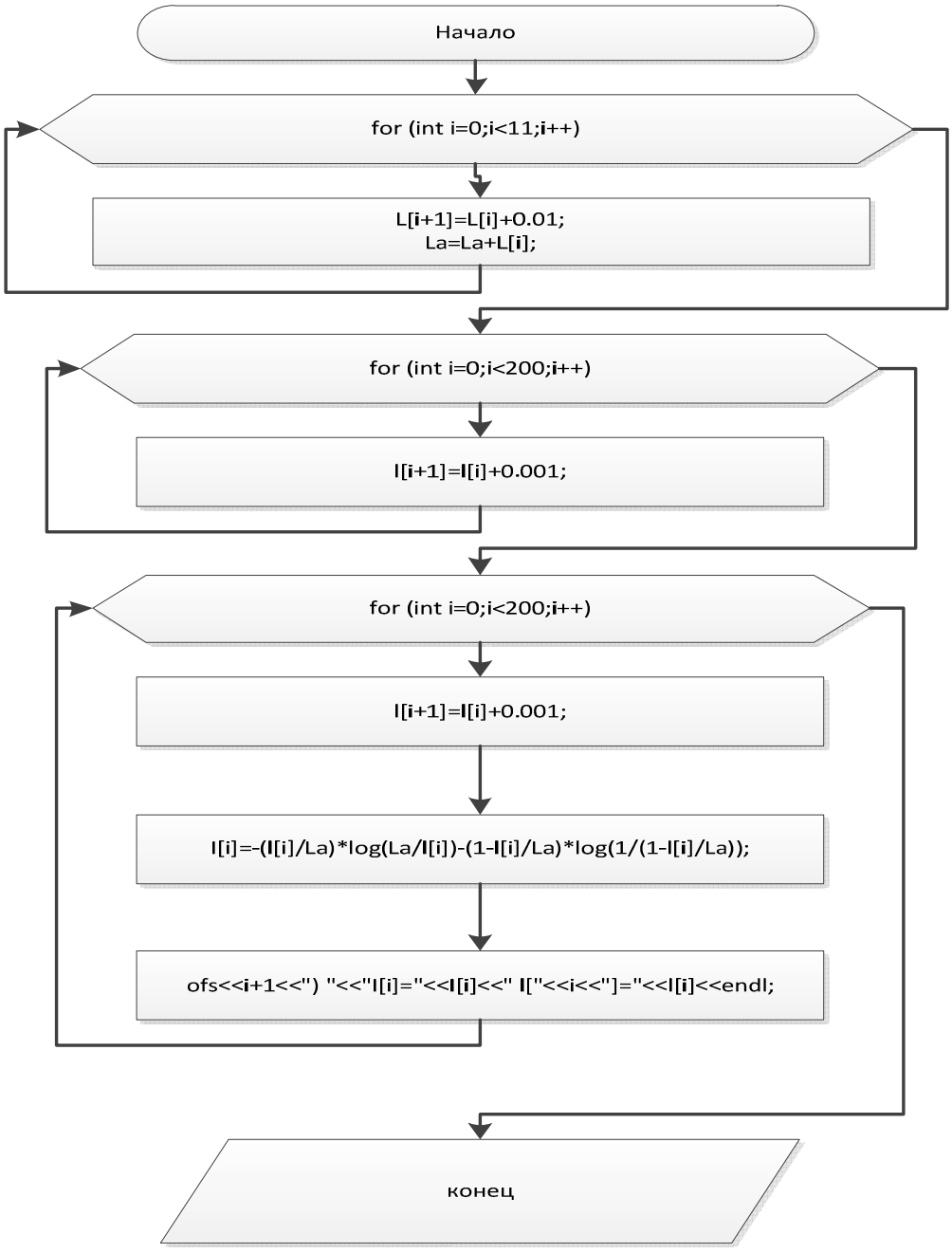

Рис. 1.

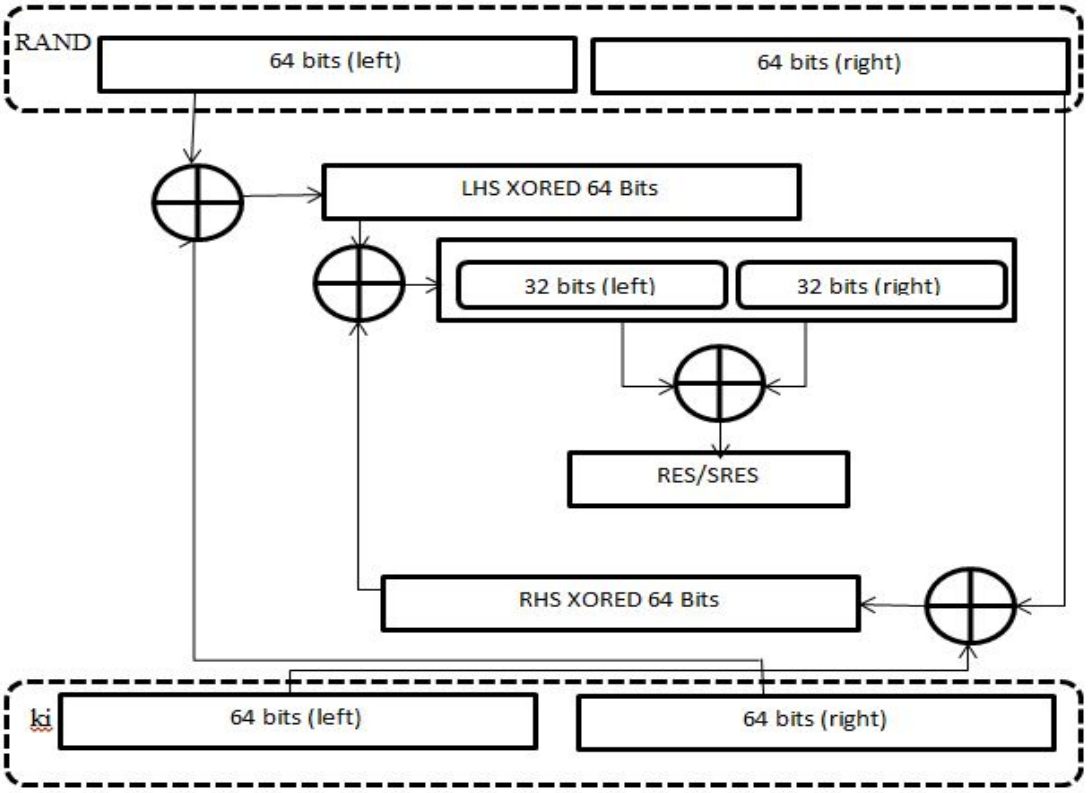
RAND
64 bits (left)
64 bits (right)
LHS XORED 64 Bits
32 bits (left)
32 bits (right)
RES/SRES
RHS XORED 64 Bits
ki
64 bits (left)
64 bits (right)

Рис. 2.

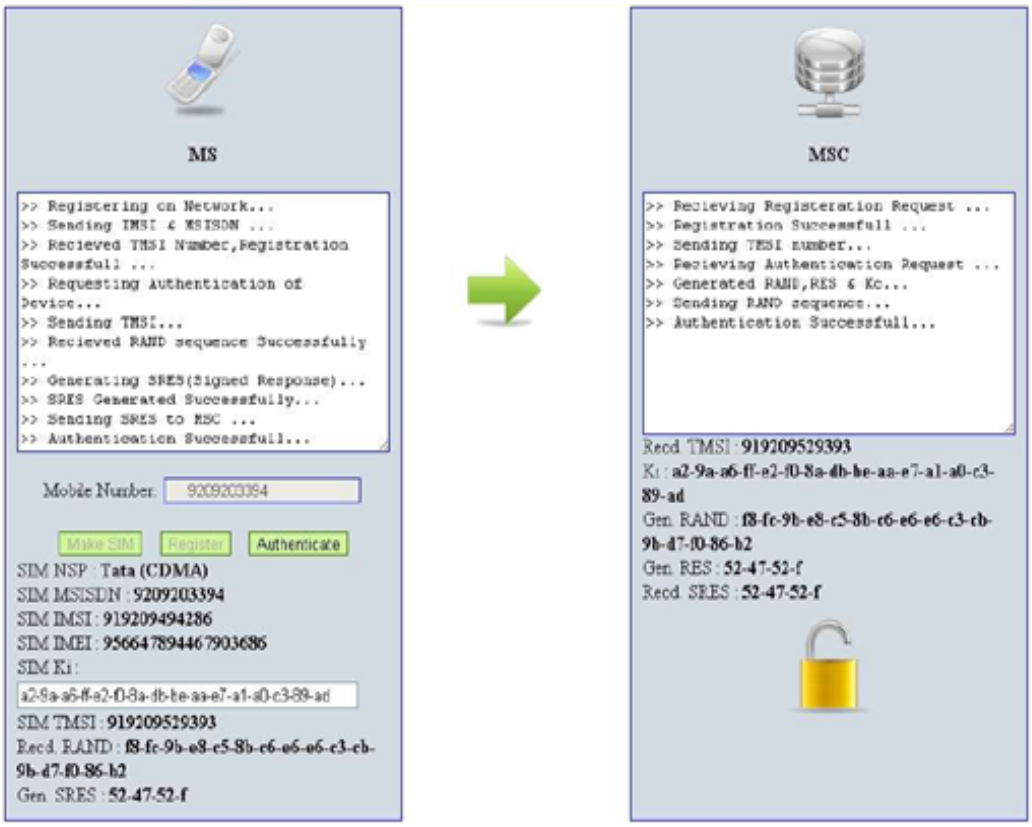
MS
>> Registering on Network...
>> Sending IMSI & MSISDN ...
>> Recieved TMSI Number,Registration Successfull ...
>> Requesting Authentication of Device...
>> Sending TMSI...
>> Recieved RAND sequence Successfully ...
>> Generating SRES(Signed Response)...
>> SRES Generated Successfully...
>> Sending SRES to MSC ...
>> Authentication Successfull...
Mobile Number: 9209203394
Make SIM
Register
Authenticate
SIM NSP : Tata (CDMA)
SIM MSISDN : 9209203394
SIM IMSI : 919209494286
SIM IMEI : 956647894467903686
SIM Ki :
a2-9a-a6-ff-a2-f0-8a-db-be-aa-e7-a1-a0-c3-89-ad
SIM TMSI : 919209529393
Recd. RAND : f8-fc-9b-e8-c5-8b-c6-e6-e6-c3-cb-9b-d7-f0-86-b2
Gen. SRES : 52-47-52-f
MSC
>> Recieving Registeration Request ...
>> Registration Successfull ...
>> Sending TMSI number...
>> Recieving Authentication Request ...
>> Generated RAND,RES & Kc...
>> Sending RAND sequence...
>> Authentication Successfull...
Recd. TMSI : 919209529393
Ki : a2-9a-a6-ff-a2-f0-8a-db-be-aa-e7-a1-a0-c3-89-ad
Gen. RAND : f8-fc-9b-e8-c5-8b-c6-e6-e6-c3-cb-9b-d7-f0-86-b2
Gen. RES : 52-47-52-f
Recd. SRES : 52-47-52-f

Рис. 3.

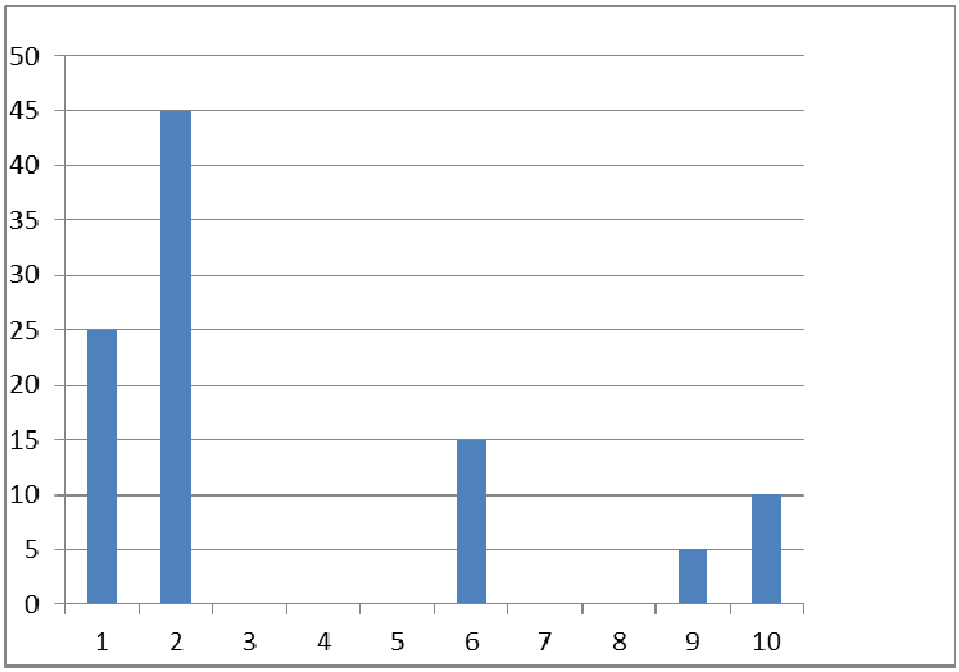

Рис. 4. Зависимость числа проникновений при шифровании в МКТС в Аммане в зависимости от используемой раздачей ключей: 1- Физическая раздача ключей. 2- Выдача общего ключа участникам взаимодействия центром выдачи ключей. 6- Предоставление центром сертификации ключей. 9- **Сеть доверия (наш алгоритм)**. 10- Метод Диффи-Хеллмана. Коды 3-5 и 7,8 существенно хуже наших требований и поэтому здесь не приведены.

При проведении эксперимента при внедрении нашего алгоритма и программы мы убедились (см. рис.4.), что число проникновений уменьшилось в среднем в 4 раза (2-9 раз) из-за целесообразного подбора ключей и их форматов применительно к МКТС медицинского центра в Аммане.

В третьей главе нами разработаны алгоритмы совершенствования управления информационными потоками и подходы в организации баз данных с целью обеспечения эффективного функционирования МКТС. Использование нашего алгоритма по минимизации маршрутизаторов позволило уменьшить число маршрутизаторов в 2-5 раз и сократить время проектирования МКТС в 3 раза. Мы модифицировали модель Хольта-Уинтерса для рядов данных с различным поведением в периодах. Такой подход позволяет не только строить более точные модели для прогнозирования развития процессов, но и осуществлять оценку объемов информационных потоков в МКТС.

Сделана постановка задачи динамического программирования для перераспределения рабочих ресурсов на различные мероприятия с целью минимизации соответствующих затрат.

Разработан алгоритм по оценке эффективности защиты на этапе расчетов и проектирования МКТС, что позволило уменьшить время в 3 раза и повысить точность оценки на 70 % при диагностике информационного канала в медицинских сетях.

При проектировании МКТС мы учитываем, что деятельность медицинского центра должна организовываться так, чтобы затраты на сопровождение были минимальны при соблюдении всех защитных мероприятий и при максимальном сохранении здоровья пациентов. Минимизация затрат нами выполняется путем подбора оптимального численного состава сотрудников центра, распределенных по различным должностям. Выполнение функций реализуется в виде проведения различных мероприятий, которые могут идти последовательно или параллельно. Для повышения вероятности выполнения всех функций время проведения мероприятий должно минимизироваться за счет перераспределения рабочих ресурсов.

В четвертой главе анализируются системы шифрования с открытым ключом, которые генерируют два цифровых ключа для каждого пользователя: один (открытый) служит для шифрования данных, другой (секретный) - для их расшифровки. С помощью секретного ключа получателя восстанавливается сеансовый (одноразовый) ключ, а затем по расшифрованному ключу расшифровывается и пересылаемый файл. Некоторые программы шифрования содержат еще одно важное средство защиты - так называемую цифровую подпись, которая удостоверяет, что файл не претерпел изменений с тех пор, как был подписан, и дает получателю информацию о том, кто именно подписал файл.

Приведем краткое описание предложенных алгоритмов шифрования с использованием ключа, пригодные для структур, которые используются в МКТС медицинского центра (рис.5).

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.

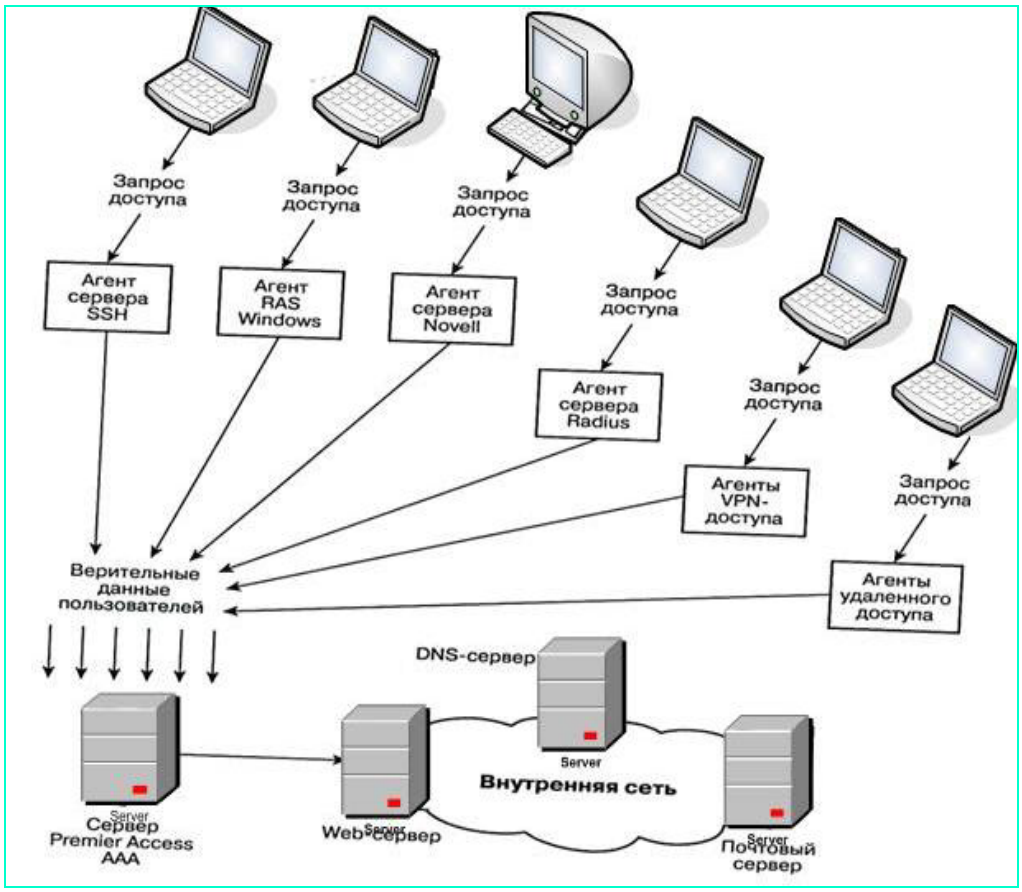

Рис. 5. Структура внутренней сети медицинского центра.

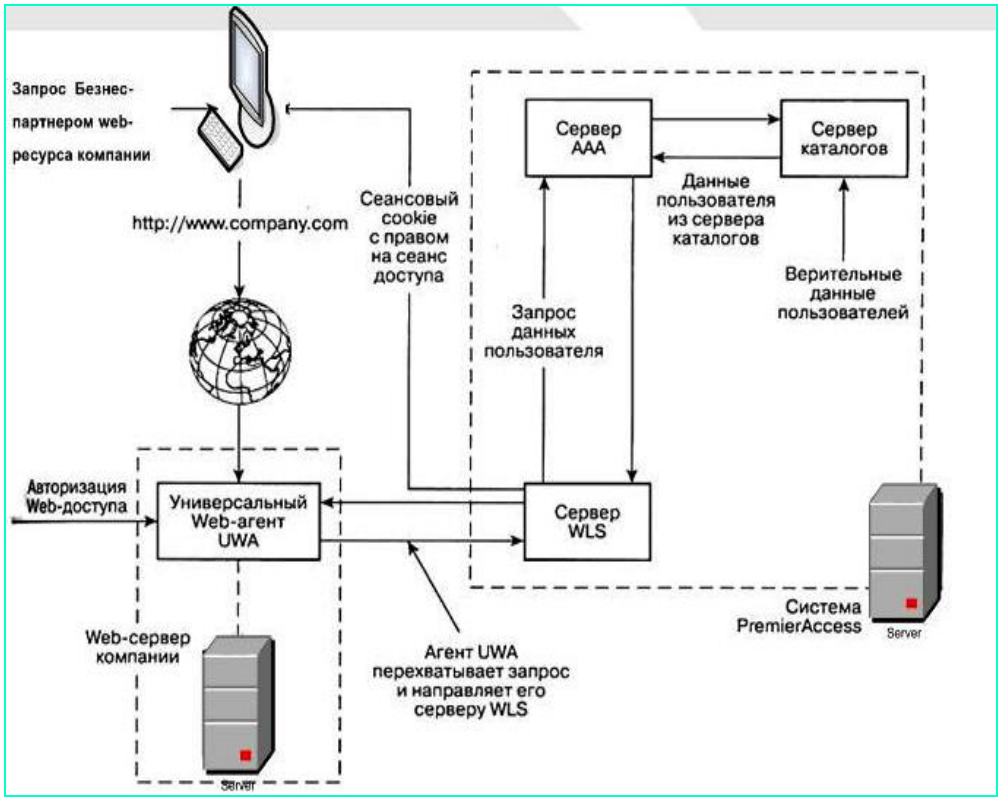

Рис. 6. Структура внешних соединений МКТС медицинского центра.

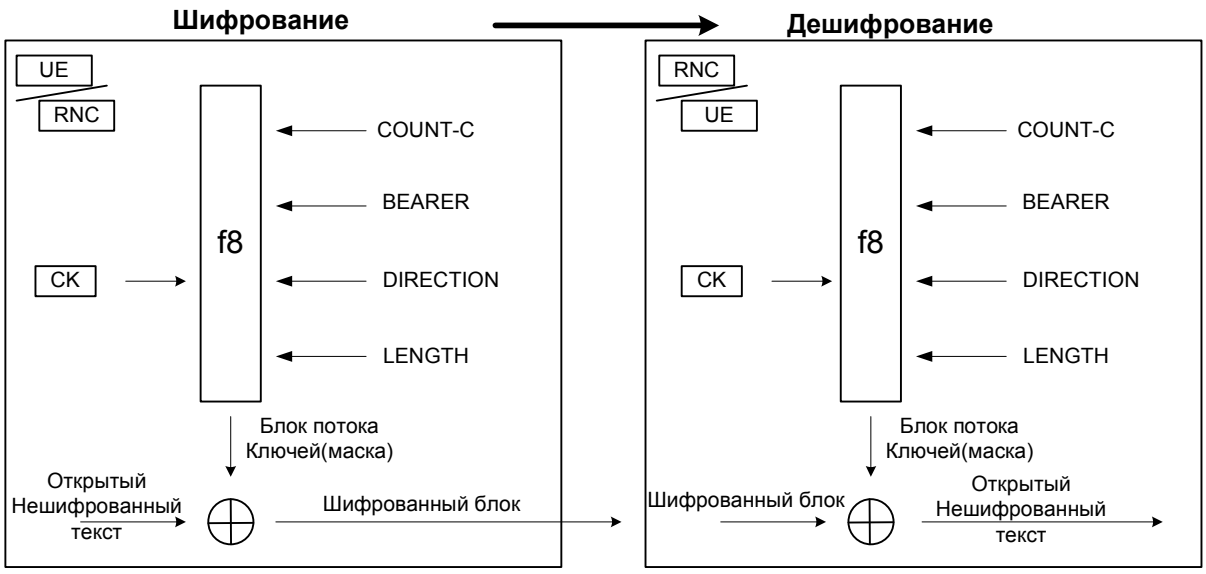

Рис. 7. Механизмы шифрования/дешифрования в МКТС.

Заключение

1. Осуществлен сравнительный анализ и выбраны методы организации хранения корпоративных данных, а также программные средства управления базами данных для МУ применительно к Иордании.
2. Проведен обзор и выделены преимущества методов математического моделирования, направленных на сопровождение и поддержку принятия управленческих решений.
3. Проанализированы основные направления создания и сопровождения медицинского центра в Аммане и отобраны методы принятия управленческих решений.
4. Применение разработанных алгоритма и программы при проведении эксперимента при внедрении показало, что число проникновений уменьшилось в среднем в 4 раза (2-9 раз) из-за целесообразного подбора ключей и их форматов применительно к МКТС медицинского центра в Аммане.
5. Разработаны алгоритмы совершенствования управления информационными потоками и подходы в организации баз данных с целью обеспечения эффективного функционирования МКТС. Использование нашего алгоритма по минимизации роутеров позволило уменьшить их число в 2-5 раз и сократить время проектирования МКТС в 3 раза.

6. Использование, разработанного автором, алгоритма по оценке эффективности защиты на этапе расчетов и проектирования МКТС позволило повысить точность оценки на 70 % и уменьшить время в 3 раза при диагностике информационного канала в медицинских сетях.

Список публикаций

(из списка ВАК)

1. Амро М.М. Системный уровень проектирования защищенных сетей / Галкин А.П., Обади Хезам, Аль-Джабери Р.Х., Ковалёв М.С. // Известия института инженерной физики. 2013. №4. - С.10-12. (25%).
2. Амро М.М. Синтез пользовательской структуры для информационной защиты сети с маршрутизаторами с использованием САПР / Галкин А.П., Альджарадат М.М., Бадван А., Дарахма Ислам., Яремченко С.В. // Известия института инженерной физики. 2014. №1. - С.11-14. (20%).
3. Амро М.М. Обоснование аппаратурных затрат на реализацию итеративного кода для обнаружения и коррекции ошибок при информационной защите / Галкин А.П., Альджарадат М.М., Дарахма Ислам // Проектирование и технология электронных средств №4,2013. – С.20-23. (30%).

(другие издания)

4. Амro М.М. projection Network-on-Chip as a System-on-Chip platform for safe information / Galkin A.P., Al-Gaberi R.H., Obadi H.M. // INDIAN SCINCE CRUISER Volume 27 Number 6 November 2013. - С.35-38. (30%).
5. Амро М.М. Повышение отказоустойчивости транспортного уровня вычислительных сетей путем реорганизации сквозной «точка-точка» множественной адресации / Галкин А.П., Альджарадат М.М., Дарахма Ислам // Перспективные технологии в средствах передачи информации / Материалы 10-й Межд. научно-технической конф. Владимир, 2013 г., т.2, - С.49-52. (30%).
6. Амро М.М. Конкурентность предприятия и его информационная защищенность / Галкин А.П., Альджарадат М.М., Дарахма Ислам, Бадван А. // Второй Российский экономический конгресс / Материалы международной Научной Конференции / Институт экономики АН РФ, Суздаль-Владимир, 2013. - С.112-115. (25%).

7. Амро М.М. Пользовательская структура для информационной защиты медицинской сети с маршрутизаторами / Галкин А.П., Дарахма Ислам., Альджарадат М.М. // Труды X Международной научной конференции «Физика и радиоэлектроника в медицине и экологии»/ Владимир-Суздаль, 2014 г. Кн. 2. - С.147-150. (30%) .
8. Амро М.М. Информационная защита отчетных материалов в корпоративной сети / Галкин А.П., Суслова Е.Г. // Материалы XI Международная научно-техническая конференция «Перспективные технологии в средствах передачи информации - ПТСПИ - Суздаль-Владимир,2015.- С. 339-342.(45%).
9. Амро М.М. Информационная защита электронного документооборота в коммуникационных сетях предприятия / Галкин А.П., Суслова Е.Г. // Материалы XI Международная научно-техническая конференция «Перспективные технологии в средствах передачи информации - ПТСПИ - Суздаль-Владимир, 2015. - С.297-299. (45%).
10. Амро М.М. Алгоритм для оценки эффективности информационной защиты медицинского центра в Иордании // Труды X11 Международной научной конференции «Физика и радиоэлектроника в медицине и экологии» / Владимир-Суздаль, книга 1, 2016. - С.328-329. (100%) .
11. Амро М.М. Улучшение аутентификации и алгоритмов шифрования в медицинских сетях Иордании /Галкин А.П. // Труды X11 Международной научной конференции «Физика и радиоэлектроника в медицине и экологии» / Владимир-Суздаль, книга 1, 2016. - С.330-332. (90%).
12. Амро М.М. Повышение эффективности информационной защиты электронного документооборота в медицинских сетях Иордании / Галкин А.П., Суслова Е.Г. // Труды X11 Международной научной конференции «Физика и радиоэлектроника в медицине и экологии» / Владимир-Суздаль, книга 1, 2016. - С.333-336. (45%).

Подписано в печать 24.10.16.
Формат 60×84/16. Усл. печ. л. 0,93. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.