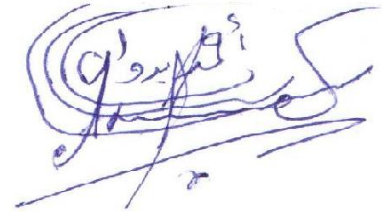


На правах рукописи



Бадван Ахмед Али

**ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ
СЕТЯХ ИОРДАНИИ**

Специальность 05.12.13 – Системы, сети и устройства
телекоммуникаций

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Владимир 2014

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 имени Александра
Григорьевича и Николая Григорьевича
Столетовых» (ВлГУ), г. Владимир

Официальные оппоненты:

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

Дерябин Вячеслав Михайлович
кандидат технических наук, доцент,
заместитель директора ОАО «Центр
автоматика», г. Владимир

Ведущая организация:

Региональный аттестационный центр
ООО «ИнфоЦентр», г. Владимир

Защита состоится « 27 » январь 2015 г. в 16.00 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 « 17 » ноябрь 2014 г.

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

Ученый секретарь диссертационного совета

доктор технических наук, профессор



А. Г. Самойлов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы.

На протяжении ряда лет во всех странах мира наблюдается тенденция стремительного развития корпоративных компьютерных телекоммуникационных сетей, современных мультимедийных средств и средств автоматизации.

С технологической точки зрения это - закономерное развитие методов использования новых информационных технологий в корпоративных сетях и на предприятиях.

Возникновение всемирной компьютерной сети открыло возможность использования информационных ресурсов и интеллектуального потенциала практически любого предприятия. Использовать открывшиеся возможности это наверно, самая актуальная задача всех телекоммуникаций.

Это вызвано рядом причин, основными среди которых можно назвать следующие:

- невозможность отрываться от производственного или иного процесса; стремление минимизировать материальные затраты на коммуникации, автоматизацию и управление.

Особую популярность это приобрело в странах, характеризующихся:

- значительными территориями; невысоким уровнем жизни; неустойчивым экономическим положением;
- наличием высокого уровня неудовлетворенного спроса на традиционные телекоммуникации.

Все эти факторы в той или иной степени относятся к Иордании, а иногда и к России.

Анализ опыта исследований и разработок европейских, американских и российских коллег показывает, что во многих странах мира уже много лет успешно развивается технологии, позволяющие, в частности, использовать Интернет для телекоммуникаций предприятий.

Очевидно, что на начальных этапах внедрения в Иордании компьютерных телекоммуникаций, могут возникнуть существенные трудности и помехи, среди которых:

-недостаточно насыщенный компьютерный парк учреждений и индивидуальных пользователей (а, часто и устаревший, без возможностей обновления);

-недостаточное развитие компьютерных телекоммуникационных сетей, их нестабильность;

-недостаточная компьютерная грамотность и информационная культура населения, что создает дополнительные психологические

барьеры в развитии передовых телекоммуникаций.

В настоящее время на рынке представлено достаточно большое число программных продуктов, предназначенных для осуществления информационного и программного обеспечения телекоммуникационных сетей. Однако 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.

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

Объект исследования - системы телекоммуникаций предприятий в государственных сетях Иордании с малыми скоростями и ёмкостями с использованием синтеза маршрутизаторов и малоразрядных кодов и защита сетей с ними от несанкционированного доступа к информации.

Предметом исследования - является разработка методики и алгоритмов обеспечения защита информации от несанкционированного доступа в системе для корпоративных и государственные сетей Иордании.

Цель работы - решение научно-технической задачи, связанной с созданием комплекса методик для повышения помехозащищенности связи и разработка 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**:

1. Выполнить оценку требований к структуре телекоммуникационных сетей предприятий и функциональным возможностям отдельных ее компонентов.

2. Рассмотреть и разработать принципы и методы поиска технических устройств несанкционированного доступа к информации, которые могут быть реализованы при ограниченных возможностях предприятий в рамках государственных сетей Иордании.

3. Разработать методику расчёта эффективности мероприятий по защите от несанкционированного доступа и оценить эффективность информационного канала с учетом защитных мероприятий.

4. Оценить показатели надежности, и уровень технического состояния защищаемого канала.

5. Разработать методики оценки государственных сетей Иордании, использующих итеративные малоразрядные коды.

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 корпоративных систем связи и защите их от несанкционированного доступа к информации.

Научная новизна работы заключается в следующем:

1. Разработаны методики и алгоритмы минимизации маршрутизаторов на этапе проектирования для конкретных предприятий и оценена целесообразность проведения защитных мероприятий с помощью наших расчётных методик.

2. Предложена методика расчета сетей и защиты информации в них и проведен синтез пользовательской структуры для информационной защиты сети для государственных сетей Иордании на основе теорий надежности и Марковских цепей.

3. Проведены математическое моделирование и практические исследования предложенных структур защиты информации в корпоративной системе связи и обосновано употребление кодов с малой разрядностью и рассчитана достоверность функционирования отказоустойчивого запоминающего устройств при информационной защите с итеративным кодом.

4. Разработан алгоритм определения состава комплекса средств защиты информации в корпоративной информационной телекоммуникационной сети (КИТС) для Иордании.

Практическая значимость работы заключается в следующем:

1. Разработаны методики и алгоритмы минимизация маршрутизаторов на этапе проектирования, что позволяет уменьшить аппаратные затраты более чем в 2 раза и сократить время проектирования сетей.

2. Предложены методики выбора контролируемых параметров по максимальным значениям (с учетом защиты канала), разработан алгоритм и программа по выбору контролируемых параметров.

3. Определен выигрыш во времени использования канала за счет уменьшения числа ошибок при отыскании проникновений и защите канала и рассчитан выигрыш во времени (в конкретных внедрениях улучшение составило 70%).

4. Доказано, что использование итеративных кодов с малой разрядностью позволяет улучшить информационную защиту (уменьшить количество по-

попыток несанкционированного доступа в сети) в 2-10 раз при ограниченных возможностях запоминающих устройств.

Основные положения, выносимые на защиту:

1. Обоснование мероприятий по защите от несанкционированного доступа и различных проникновений в информационные сети Иордании.
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 синтеза маршрутизаторов.

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

В диссертации использованы результаты исследований и 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 на предприятиях в виде программных продуктов по защите информации в каналах, алгоритмов и методик в ОАО «РИК», в ОАО «Владремстрой» (г. Владимир), и в ООО «Электроприбор» (г. Москва), что подтверждено соответствующими документами.

Апробация работы. Основные научные и практические результаты работы докладывались и обсуждались на 5-ти международных конференциях, в том числе: 9-й, 10-й международных научно технической конференции «Перспективные технологии в средствах передачи информации», г. Владимир, 2011, 2013гг.; Международной конференции НПК «Факторы развития региональных рынков», г. Владимир, 2011 г.; X международной научно-технической конференции «Физика и радиоэлектроника в медицине и экологии» (ФРЭМЭ-2012), г. Владимир, 2012г.; 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 статьях и трудах НТК (из них 3 из списка ВАК), в отчетах Госбюджетных НИР кафедры радиотехники и радиосистем №118 (2011-2013гг.). На международных научно-технических конференциях и семинарах сделано 5 докладов и сообщений.

Структура и объём диссертации. Диссертация состоит из введения, трёх глав, заключения и библиографического списка, включающего 118 наименований (130 стр. основного текста, 20 рисунков и 11 таблиц).

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность работы, сформулированы цели и задача исследований с учетом особенностей 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. Рассматривается несанкционированный доступ к информации в корпоративных сетях, анализ технических каналов корпоративных сетей по несанкционированному доступу и защите от него, информационная безопасность и риски при проектировании, финансовая устойчивость и информационная безопасность предприятия.

Даны классификация и характеристика технических каналов утечки информации, обрабатываемой техническими средствами, передаваемой по каналам связи. Рассмотрены защита телекоммуникаций учреждений и предприятий с особенностями, свойственными для Иордании, информационные сети Иордании, 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, особенности информационной безопасности государственных сетей Иордании, оценка эффективности информационного канала с учётом защитных мероприятий.

Во второй главе в диссертации рассматривается ущерб от несанкционированного доступа в корпоративных сетях и защита от него, в частности, приводятся данные по ущербу мировой экономики от несанкционированных проникновений в информационные сети, информационные атаки на финансы, универсальные угрозы для корпоративных систем.

Отдельно рассматриваются вопросы поиска технических устройств пе-

рехвата информации в учреждениях и предприятиях.

Рассмотрены методики для расчётов целесообразности организации защиты информации от несанкционированного доступа с целью улучшения телекоммуникационных возможностей предприятий.

Проведена оценка эффективности мероприятий по защите корпоративных сетей Иордании от несанкционированного доступа и оценка эффективности информационного канала с учетом защитных мероприятий. Найдена зависимость эффективности корпоративной сети связи Иордании от срывов. Прделана минимизация маршрутизаторов при обеспечении информационной защиты в сетях для государственных сетей Иордании.

Третья глава посвящена вопросам целесообразности организации защиты информации от несанкционированного доступа и минимизации маршрутизаторов при обеспечения информационной защиты в сетях для государственных сетей Иордании.

Рассмотрим алгоритм поиска и построения маршрутизаторов для обеспечения информационной защиты в сетях. Сначала построим матрицу уровней L . Уровнями будем называть x и y координаты, на которых лежат ядра(либо проводное соединение, либо создающее беспроводное распространение информации, либо маршрутизаторы). В строках матрицы L будут лежать x -ые уровни, соответственно в столбцах y -ые уровни. Элементы матрицы, это ядра - лежащие на соответствующих уровнях(рис1).

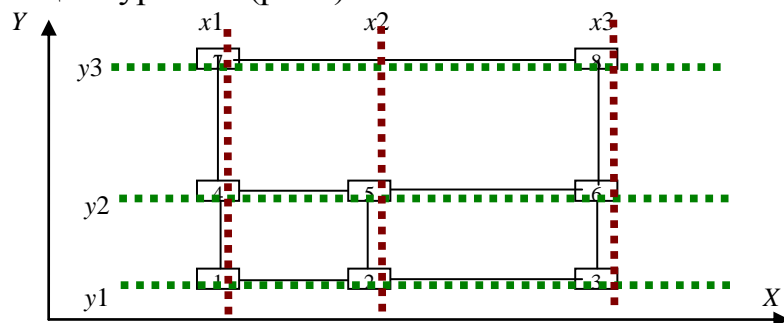


Рис 1. Уровни ядер в сети.

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

Перебираем все ядра.

1. Возьмем i -е ядро
2. Проверяем, если оно не принадлежит ни одному из уровней, или уровни еще не созданы. Тогда создаем новый уровень, это будет новая строка в матрице L .

3. Далее для x -координаты находим все остальные ядра, лежащие на этом уровне. Те x координаты, которых равны (см. Рис 1).

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

После построения матрицы уровней L , находим начало будущих маршрутизаторов.

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

Блок-схема нашего алгоритма показана на рис 2.

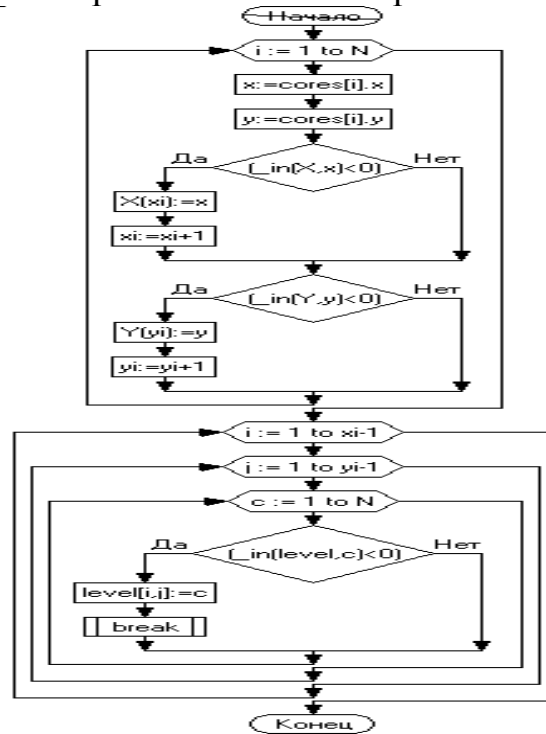


Рис.2. Блок-схема алгоритма

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

Для нахождения “угловых ядер”, возьмем ядро из матрицы L с индексами (i, j) , где i – это индекс по уровню x , а j – по y . И проверим есть ли у него связь с $L(i + 1, j)$ и $L(i, j + 1)$, если есть то ядро $L(i, j)$ и есть “угловая точка” а, соответственно $L(i + 1, j)$ и $L(i, j + 1)$, c и b (см рис.3). Теперь остается найти точку d .

Для этого начиная с $L(i + 1, j)$ двигаемся вниз, до уровня $L(i, j + 1)$ и если находим ядро $L(i + 1, j + k)$ связанное с $L(i, j + 1)$, это и есть искомая точка d . Если на уровне $i + 1$ не нашли точку d , переходим к следующему уровню $i + 2$ и т.д. пока не будет найдена точка или же не закончатся ядра. Индексы i, j пробегают от 1 до $X - 1$ и от 1 до $Y - 1$, соответственно. Возьмем ядро 1. Оно находится на уровне x_1 и y_1 . Ищем его соседей с лева и сверху. Это ядра 4 и 2 если с ними есть связь, то это возможно маршрутизатор. И начинаем двигаться от ядра 4, находящимся на уровне x_1, y_2

вниз до уровня на котором находится ядро 2 те x_2 . Там есть ядро 5, которое связано с 2 и 4, маршрутизатор построен, и он состоит из ядер 1,2,4,5. По аналогии строим маршрутизатор 2,3,5,6 и 4,6,7,8.

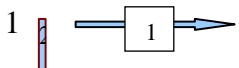



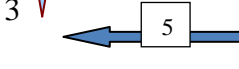
	y1	y2	y3
x1	1 	4 	7
x2	2 	5 	0
x3	3 	6	8

Рис. 3. Номера на стрелках указывают порядок действий.

После построения маршрутизаторов получаем массив маршрутизаторов R . Каждый $R(i)$ элемент которого, маршрутизатор и ядра, которые входят в него. Каждый маршрутизатор так же будет иметь начальные координаты x, y - это координаты левого нижнего угла, высоту h и ширину w .

По вышеприведенному алгоритму строятся все возможные маршрутизаторы. Минимизация ресурсов маршрутизатора приводит к сокращению статического расхода энергии и облегчению проектирования и верификации. Мы можем уменьшить их количество путем объединения соседних маршрутизаторов. При этом объединении нужно проводить таким образом, чтобы не пропадали ядра (см. пример на рис.4). И длина пути не оказалась больше максимально разрешенной длины пути D .

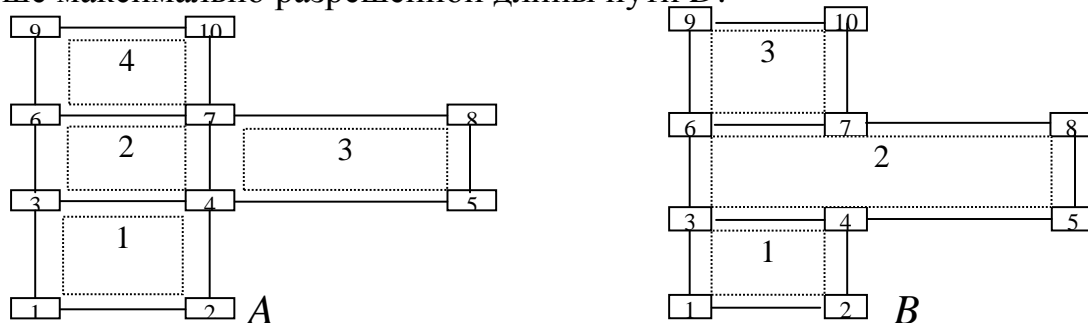


Рис.4. Объединение маршрутизаторов. A — до объединения, B — после.

Вспомогательные функции :

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

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

Маршрутизаторы будем объединять следующим образом.

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

Блок-схема алгоритма построения маршрутизаторов и их минимизации.

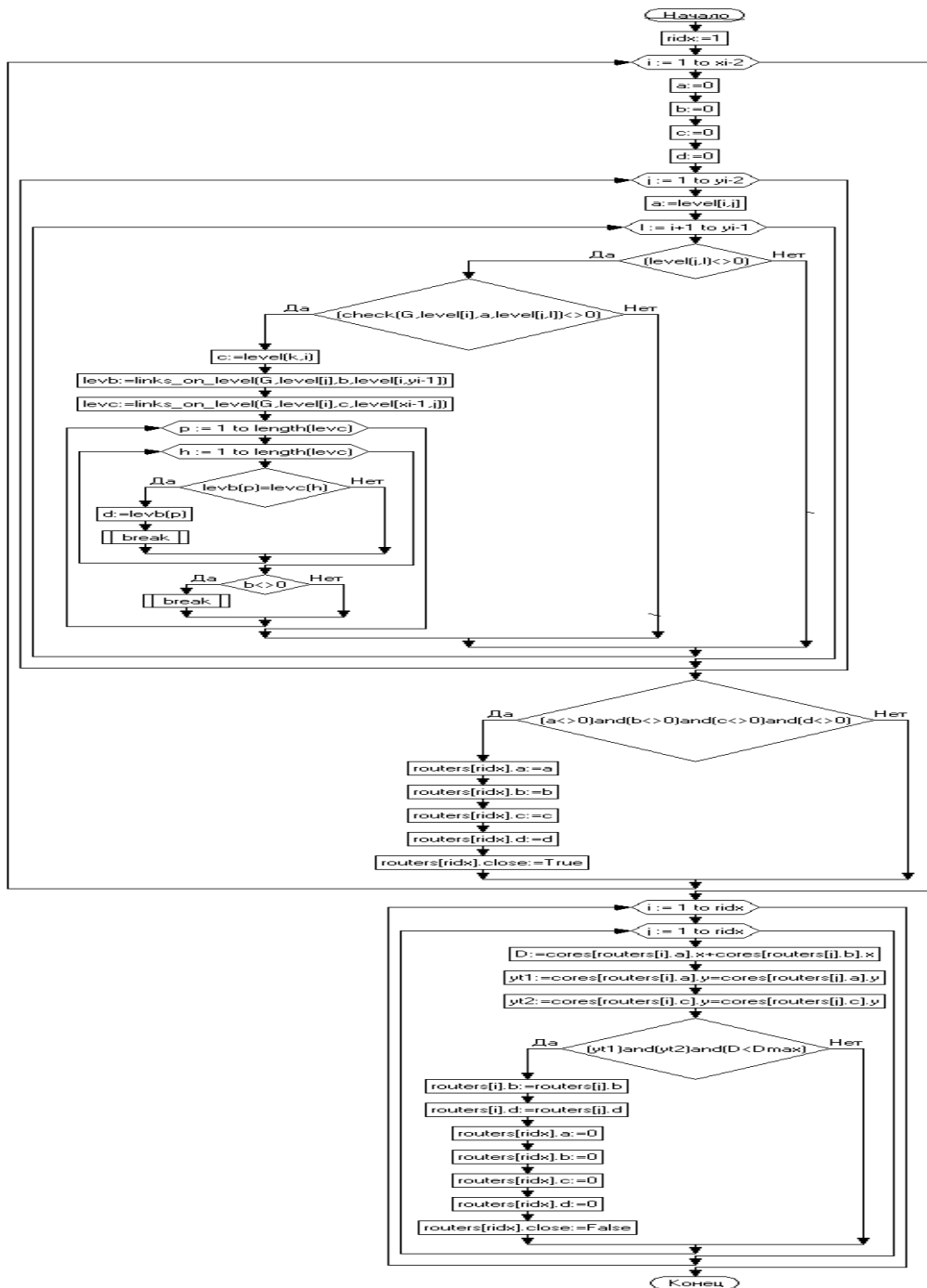


Рис.5. Алгоритм построения маршрутизаторов и их минимизации.

Возьмем $R(i)$ маршрутизатор и его соседей, если их ядра лежат на одинаковых x или y уровнях, тогда эти маршрутизаторы можно объединить в один. Т.е. один маршрутизатор является продолжением другого. Например, можно объединить маршрутизаторы 2 и 3, так как 3,4,5 и 6,7,8 образующие эти маршрутизаторы лежат на одинаковых y уровнях. При этом ядра 4,7 останутся в маршрутизаторах 4,1. Но нельзя объединить маршрутизаторы 1,2,4 так как при этом произойдет исключение из топологии ядер 3 и 6.

Итак, после объединения получаем минимизированное количество

маршрутизаторов.

Нами предложено, что у каждого ядра есть только один порт ввода/вывода (*I/O*), который должен быть присоединен к единственному порту маршрутизатора. Можно тривиально допустить ядра с многочисленными портами ввода/вывода, которые должны быть преобразованы в определенные маршрутизаторы.

Защищать информационную систему имеет смысл только комплексно, т.е. одновременно от всех угроз, как программное обеспечение, аппаратные средства, так и инфраструктуру.

Построим такую систему защиты (*СЗ*) путем подбора оптимального количества наиболее эффективных мероприятий, которые смогли бы обеспечить защиту целостности, конфиденциальности, полноты и доступности информации заданным качеством.

Обобщенный алгоритм поиска оптимального состава *СЗ*, противодействующего атаке злоумышленника при реализации его конкретной цели в КИТС приведен на рис.6

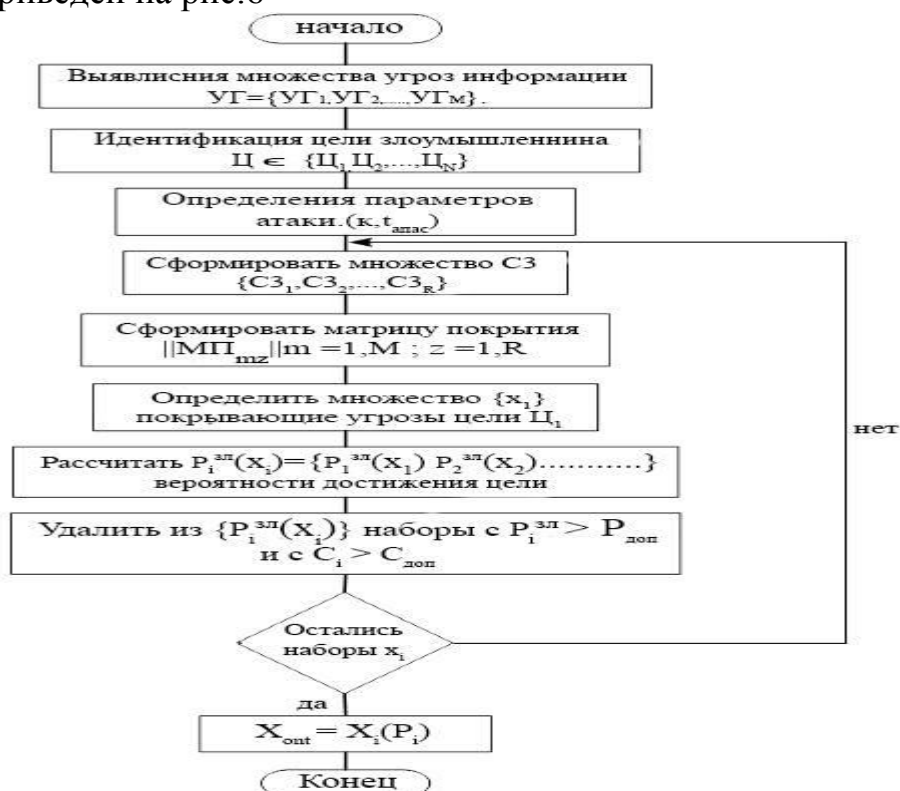


Рис.6. Схема алгоритма определения состава комплекса средств защиты информации в КИТС.

Основная роль транспортного уровня SCTP (Stream Control Transmission Protocol - протокол управления потоковой передачей) состоит в организации сквозной (точка-точка) коммуникационной службы между двумя или несколькими приложениями, работающими на разных хостах. Он изолирует приложения от специфики сети, соединяющей хосты, и предоставляет разработчикам приложений простой интерфейс.

Другим важным качеством SCTP является поддержка множественных адресаций хостов, позволяющая создавать конечные точки SCTP с множеством IP-адресов. Поддержка множественных адресаций хостов повышает уровень «живучести» сессий в случаях возникновения сбоев в сети. В традиционных одноадресных сеансах отказ в соединении с ЛВС может изолировать конечную точку, а сбой в работе магистральной сети может привести к временным проблемам на транспортном уровне, пока протокол маршрутизации IP не найдет пути в обход сбойного участка.

Для повышения уровня безопасности требуется, чтобы некоторые отклики передавались по адресу, указанному в поле отправителя сообщения, вызвавшего отклик. Например, когда сервер получает блок INIT от клиента для инициирования SCTP-ассоциации, сервер всегда будет передавать блок INIT АСК по адресу отправителя в заголовке IP блока INIT. Пример, топология сети с множественной адресацией показана на рис. 7.

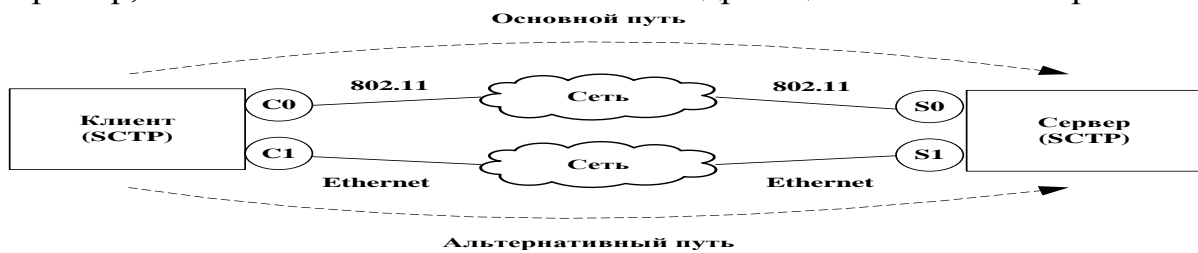


Рис. 7. Топология сети с множественной адресацией.

Механизм отказоустойчивости в протоколе SCTP.

Каждая конечная точка использует скрытые и заданные зонды для динамической поддержки информации о достижимости IP-адресов клиентов. В случае когда количество выдаваемых ошибок превышает допустимый порог, называемый PMR (Path. Max. Retrans - Максимальное количество перезапусков), система выдаёт «отказ». Рис. 8. иллюстрирует механизм работы системы отказоустойчивости для конечных точек n . Соединение начинается в фазе 1, где конечная точка D_i является основной, находится в активном состоянии, и все новые данные отправляются в D_i . Когда D_i даёт сбой, происходит «отказ» и соединение направляется в фазу 2.

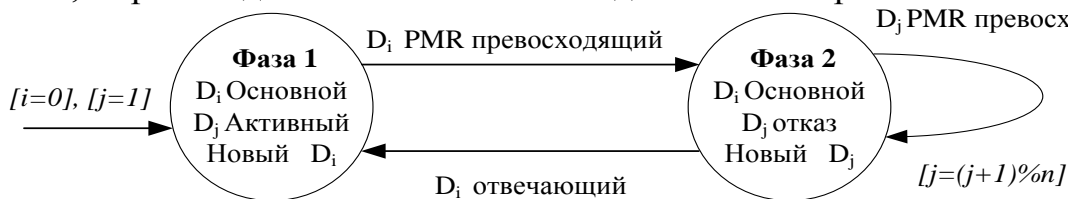


Рис. 8. Автомат существующего механизма переключения.

В фазе 2 D_i остаётся основной точкой назначения, но в состоянии отказа, все новые данные перенаправляются в альтернативную точку D_j . Если существует более одного адреса альтернативных точек, то отбор осуществляется по циклическому методу. В случае если в альтернативной точке количество ошибок вновь превышает допустимый порог PMR, соединение остаётся в фазе 2. При получении отклика от D_i , отказ прекращается, и соединение возвращается в фазу 1.

Время обнаружения отказа зависит от трёх параметров:

- 1) RTO минимальное (время реагирования);
- 2) RTO максимальное;
- 3) PMR=5;

Сокращение PMR уменьшает время обнаружения ошибок и увеличивает вероятность ложных отказов, что не рекомендуется расценивать как недостаток системы, а наоборот может улучшить характеристики канала. Вероятно, механизму отказоустойчивости не следует возвращать соединение к фазе 1 в случае получения отклика по основному каналу, а продолжать передачу информации по альтернативному, тем самым экономя время RTO и сводя PMR к нулю.

При использовании итеративных кодов в запоминающих устройствах телекоммуникационных сетей при их информационной защите необходимо убедиться в достоверности. Нами разработана методика определения достоверности функционирования.

Оценку достоверности функционирования отказоустойчивых (информационно защищенных) запоминающих устройств (ЗУ) рассмотрим на примере для четырех информационных разрядов с использованием первого варианта кодирования. В этом случае: $r=k+4=8$; $n=k+r=12$.

Предположим, что емкость накопителя M составляет 10000 4-х разрядных ячеек памяти, а интенсивность отказа одного логического элемента равна $\lambda_i = 1 \cdot 10^{-9} \text{ 1/ч}$, ($p(t) = e^{-10^{-9}t}$).

Вероятность безотказной работы накопителя по одному выходу равна: $p1(t) = p(t)^{6M}$.

Аппаратурные затраты на построение декодирующего устройства составят 30000 двухвходовых логических элемента.

Достоверность функционирования отказоустойчивого ЗУ оценим используя выражение:

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

Проведем оценку влияния кратности исправляемой ошибки аппаратурные затраты и достоверность функционирования устройств памяти при реализации предлагаемых подходов кодирования информации.

Сравнительную оценку достоверности функционирования электронных устройств в зависимости от кратности исправляемой ошибки.

Исходные данные:

- количество информационных разрядов $k=4$;
- количество контрольных разрядов $R=8$;
- вероятность безотказной работы одного простейшего логического элемента $P(t) = e^{-10^{-9}t}$;
- емкость накопителя $M = 6000$;

– вероятность безотказной работы одного выхода $P1(t) = P(t)^{6M}$.

Проведем сравнительную оценку достоверности функционирования.

В результате получим графические зависимости (см. Рис.9), отображающий зависимость достоверности функционирования запоминающего устройства от времени.

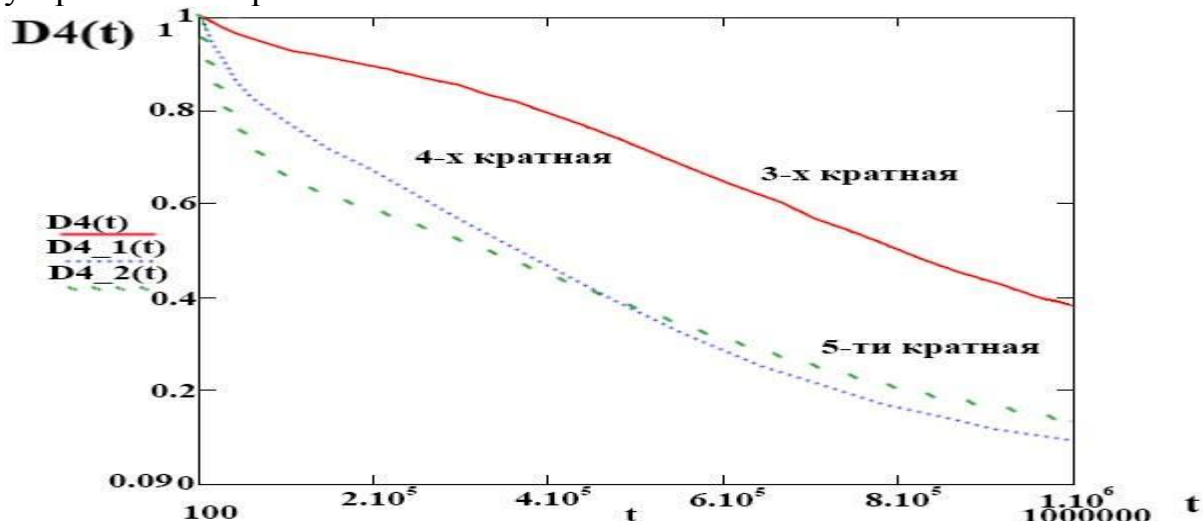


Рис.9. Сравнительная оценка достоверности функционирования от кратности исправляемой ошибки.

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

В целях защиты сети от несанкционированного доступа создается подсистема, позволяющая решать задачи:

1. Распределение маршрутизатора: Устройство локализует маршрутизаторы в узлах графа пересечения канала для общей топологической структуры системного уровня. Ребра различных ядер формируют ребра графа пересечения канала. Пересечение двух ребер в углах ядер обозначает вершины в графе.
2. Ядро к преобразованию маршрутизатора: Как следующий шаг, устройство соединяет каждое ядро с одним из маршрутизаторов на его четырех ребрах. Генерирование маршрута и синтез топологии: Затем устройство генерирует маршруты для каждого из путей. Представлен алгоритм приближения, который маршрутизирует пути и синтезирует топологию таким образом, чтобы расход энергии был минимален, и чтобы необходимое число маршрутизаторов было бы максимум в 2 раза больше, чем в оптимальном решении.
3. Слияние маршрутизатора: предпоследний шаг в стадии синтеза соединяет близко находящиеся маршрутизаторы в один маршрутизатор, при условии, что ограничения длины канала передачи данных не нарушены.
4. Анализ зависания: заключительный этап в потоке синтеза анализирует произведенную топологию на потенциальные зависания. Поскольку маршруты различных путей определены в стадии проектирования, можно обнаружить и уменьшить потенциальные зависания в синтезируемой структуре.

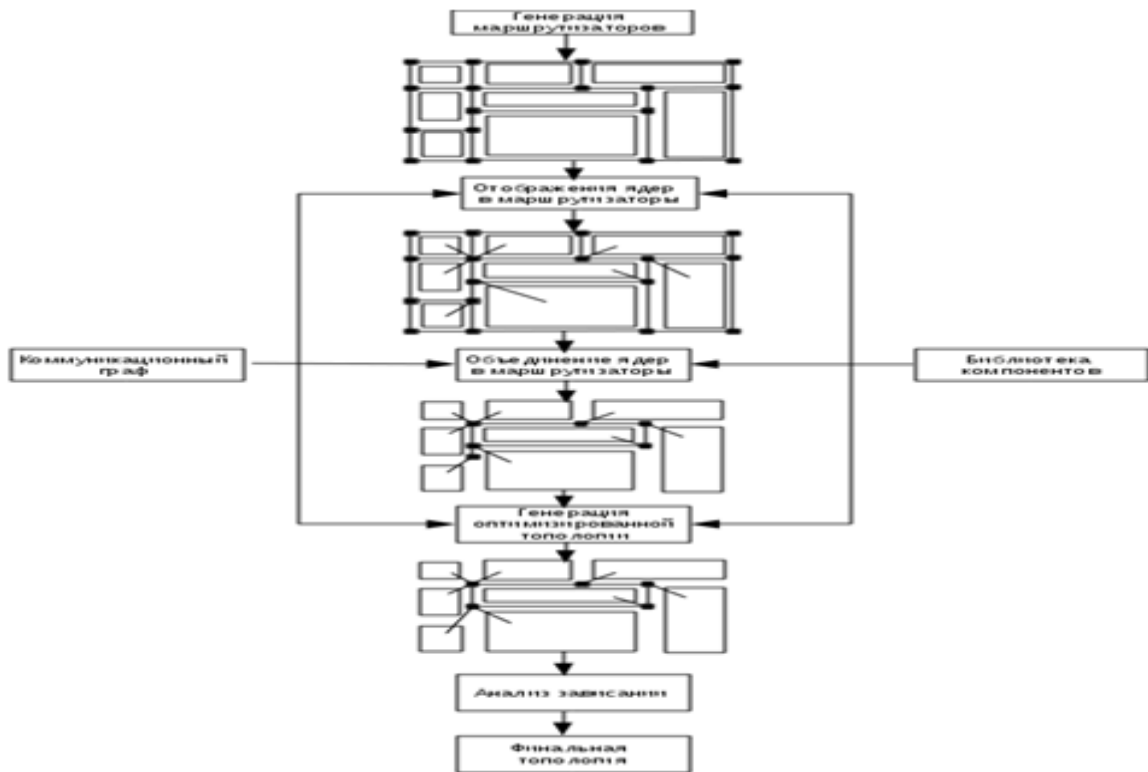


Рис. 10. Схематичное проектирование специализированного приложения. Структура комплекса представлена на рис.11.

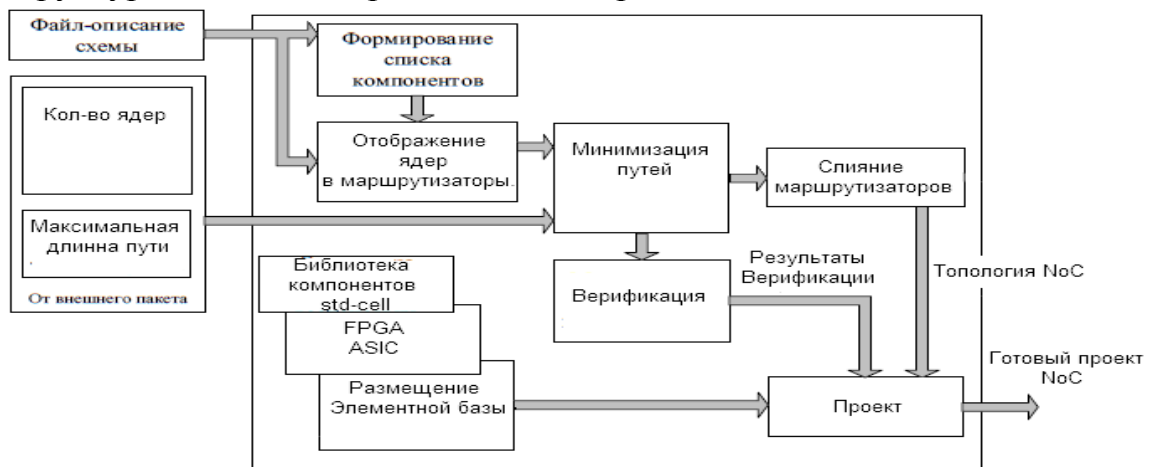


Рис.11. Структура комплекс представляет собой подсистему САПР, реализованную по агрегатному принципу на основе открытой архитектуры.

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

1. Анализ объекта защиты.
2. Генерация топологии защищаемой сети.
3. Поиск неисправности или несанкционированного проникновения в сеть.
4. Экспорт в САПР.

Основные результаты и выводы

В ходе проведенных исследований получены следующие основные результаты.

1. Рассмотрены различные пути обеспечения информационной защиты предприятий с целью ее улучшения при учете особенностей Иордании.
2. Определен выигрыш во времени использования канала за счет уменьшения числа ошибок при отыскании проникновений, и защите канала и рассчитан выигрыш во времени (в конкретных внедрениях улучшение составило 70%).
3. Предложена методика выбора контролируемых параметров по максимальным значениям (с учетом защиты канала), разработан выбор контролируемых параметров по заданному коэффициенту готовности и проведен выбор контролируемых параметров по максимальному значению вероятности безотказной работы после проведения диагностики с оценкой оптимального времени между проведением функциональных проверок информационного канала.
4. Предложены пути оптимального выбора параметров с малоразрядными кодами для защиты каналов предприятий и учреждений Иордании с целью сокращения аппаратных расходов, из-за устаревшего сетевого оборудования (которое в ближайшее время не будет обновляться).
5. Разработан алгоритм и программа по выбору контролируемых параметров по максимальным значениям важнейших характеристик корпоративных сетей.
6. Сделаны оценки по различным критериям и разработаны рекомендации по внедрению в системе связи средств защиты информации и определен выигрыш во времени использования канала за счет уменьшения числа ошибок при отыскании проникновений и защите канала.
7. Доказано, что использование итеративных кодов с малой разрядностью позволяет улучшить информационную защиту (достоверность) в 2-10 раз при ограниченных возможностях запоминающих устройств.
8. Разработаны методики и алгоритмы минимизация маршрутизаторов на этапе проектирования что позволяет уменьшить аппаратные затраты более чем в 2 раза.
9. Разработан синтез пользовательской структуры для информационной защиты сети с маршрутизаторами с использованием САПР для Иордании, что позволяет сократить время (проектирование) на 20%.
10. Разработан алгоритм для определения состава комплекса средств защиты информации в корпоративной информационной телекоммуникационной сети (КИТС) для Иордании.

Полученные научные результаты свидетельствуют о решении научной проблемы, связанной с достижением качественно нового уровня обеспечения отказоустойчивости корпоративных сетей, необходимого для поддержания их живучести в экстремальных условиях работы.

Решение рассматриваемой научной задачи имеет важное значение для Иордании, поскольку улучшает достоверность функционирования телекоммуникационных государственных сетей Иордании при ограниченных затратах.

Разработанные методики и алгоритмы позволяют обеспечить комплексное решение научной задачи повышение вероятности безотказной работы и достоверности функционирования телекоммуникационных устройств, работающих в реальном масштабе времени для повышения информационной защищенности телекоммуникационных сетей.

Список основных научных работ, опубликованных по теме диссертации

Статьи в журналах из перечня ВАК РФ

1. Бадван Ахмед. Улучшение отказоустойчивости вычислительных сетей при множественной адресации / Бадван Ахмед, А.П. Галкин, О. Тахаан, С.В. Яремченко // Известия института инженерной физики. - 2012. - №3, - С. 22-24.
2. Бадван Ахмед. Минимизация при обеспечении информационной защиты в сетях / Бадван Ахмед, А.П. Галкин, М.М. Али Альджарадат, И. Дарахма, С.В. Яремченко // Известия института инженерной физики. - 2013. - №1, - С. 2-4.
3. Бадван Ахмед. Синтез пользовательской структуры для информационной защиты сети с маршрутизаторами с использованием / Бадван Ахмед, А.П. Галкин, М.М. Али Альджарадат, И. Дарахма, С.В. Яремченко, Амро Мохаммад Махмуд // Известия института инженерной физики. - 2014. - №1, - С. 11-14.

Материалы конференций

4. Бадван Ахмед. Защита от угроз информационной безопасности в телекоммуникационных сетях / Бадван Ахмед, А.П. Галкин, О. Тахаан // Перспективные технологии в средствах передачи информации / Материалы 9-й Межд. научно-технической конференция. Владимир-Суздаль, - 2011. - Т.1. - С. 42-45.
5. Бадван Ахмед. Улучшение экономических характеристик при повышении отказоустойчивости транспортного уровня вычислительных сетей / Бадван Ахмед, А.П. Галкин, О. Тахаан, И.Н. Кирсенко // Факторы развития региональных рынков / Материалы международной научн.- практич. конф., Владимир, - 2011. - С. 23-26.
6. Бадван Ахмед. Когнитивное радио - важное направление в инновационном развитии здравоохранении / Бадван Ахмед, А.П. Галкин, Обади Хезам., Аль-Джабери Рамзи // Труды X Международной научной конференции «Физика и радиоэлектроника в медицине и экологии» / Владимир-Суздаль, - 2012. - книга 2, - С. 176-178.
7. Бадван Ахмед. Техника - экономическое обоснование беспроводных сетей для инновационного развития регионов / Бадван Ахмед, А.П. Галкин, Обади Хезам // Управление инновационными процессами развития регио-

на / Материалы международной научн.- практич. конференции, - Владимир, - 2012.- С.47-51.

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

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

10. Бадван Ахмед. Конкурентность предприятия и его информационная защищенность / Бадван Ахмед, А.П. Галкин, М.М. Альджарадат, М.М. Амро, И. Дарахма // Материалы второго российского экономического конгресса. - Институт экономики АН РФ, - Владимир-Суздаль, - 2013. - С. 112-114.

11. Бадван Ахмед. Повышение эффективности сложных РЭС. Отчёт по госбюджетной НИР №118, - 2011-2013 г.

Подписано в печать

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.