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

Бадван Ахмед Али

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ ИОРДАНИИ

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

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук,
профессор Галкин А.П.

Владимир 2014

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ

AOL - служба America Online

АК - абонентский комплект

АКС - аппаратура конфиденциальной связи

АМЗК - автоматические мероприятия по защите канала

АНБ - Агентство национальной безопасности (США)

АСР - автоматизированные системы расчетов Platex

ВСС - взаимоувязанная система связи

ВТСС - вспомогательные технические средства и системы

ЕПГУ - единый портал госуслуг

ЗМ – защитных мероприятий

ЗСПД - защищенной сети передачи данных

ЗУ - запоминающее устройство

ИБ – информационная безопасность

ИС – информационная система

ИТС - информационная телекоммуникационная сеть

КИТС - корпоративная информационная телекоммуникационная сеть

КПИ - коэффициент потерь информации

КПК – карманный ПК

КС - канал связи

ЛВС - локальные вычислительные сети

МЭДО - система межведомственного электронного документооборота

НСД - несанкционированный доступ

ОЗУ - оперативное запоминающее устройство

ОУ - объединяющее устройство

ПГУ - портал государственных услуг

ПИП - повторных информационных потоков

ПК - персональный компьютер

ПОИБ - подсистем обеспечения информационной безопасности

ПО - программное обеспечение

ПЭВМ - персональная ЭВМ (ПК)

RTO - время реагирования

РЭО - радиоэлектронная обстановка

РЭС - радиоэлектронные средства (радиоэлектронная система)

PMR - максимальное количество перезапусков (Path. Max. Retrans)

СЗ - множество средств защиты

САПР - система автоматизированного проектирования

СЗИ - система защиты информации

SCTP - протокол управления потоковой передачей (Stream Control Transmission Protocol)

СМЭВ - системы межведомственного электронного взаимодействия

ТКУИ - технический канал утечки информации

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

ТСР - технические средства разведки

УГ - множество всех возможных угроз информации в сети

ГС - государственные сети

Введение

Актуальность проблемы

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

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 устаревщий, 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 предприятий и государственных сетей, а также особенности состояния сетевых коммуникаций в ее регионах, представляется чрезвычайно актуальной в современных условиях.

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

Предметом исследования - является разработка методик и алгоритмов обеспечения защиты информации от несанкционированного доступа в корпоративные и государственные сети 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, теории нелинейных динамических систем, 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 минимизация 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 инфрмации в корпоративной информационной телекоммуникационной сети (КИТС) для Иордании.

Практическая значимость работы заключается в следующем:
1.Разработаны методики и алгоритмы минимизации маршрутизаторов на этапе проектирования, что позволяет уменьшить аппаратурные 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 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.

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 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: 9-й международной научно технической конференции «Перспективные технологии в средствах передачи информации», г. Владимир, 2011г.; 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 (2011-2013 гг.). 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 и 7 приложений. Объём диссертации: 130 страниц основного текста, 20 рисунков и 11 таблиц.

ГЛАВА 1. НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ

1.1 Информационные сети Иордании

Информационные сети: Эти сети, предназначенные для обработки, хранения и передачи данных. Информационные сети состоит из:

-абонентских и административных систем;

-связывающей их коммуникационной сети;

В зависимости от расстояния между абонентскими системами, информационные сети подразделяются: на глобальные, территориальные и локальные. Различают универсальные и специализированные информационные сети[1,2,4,103-115].

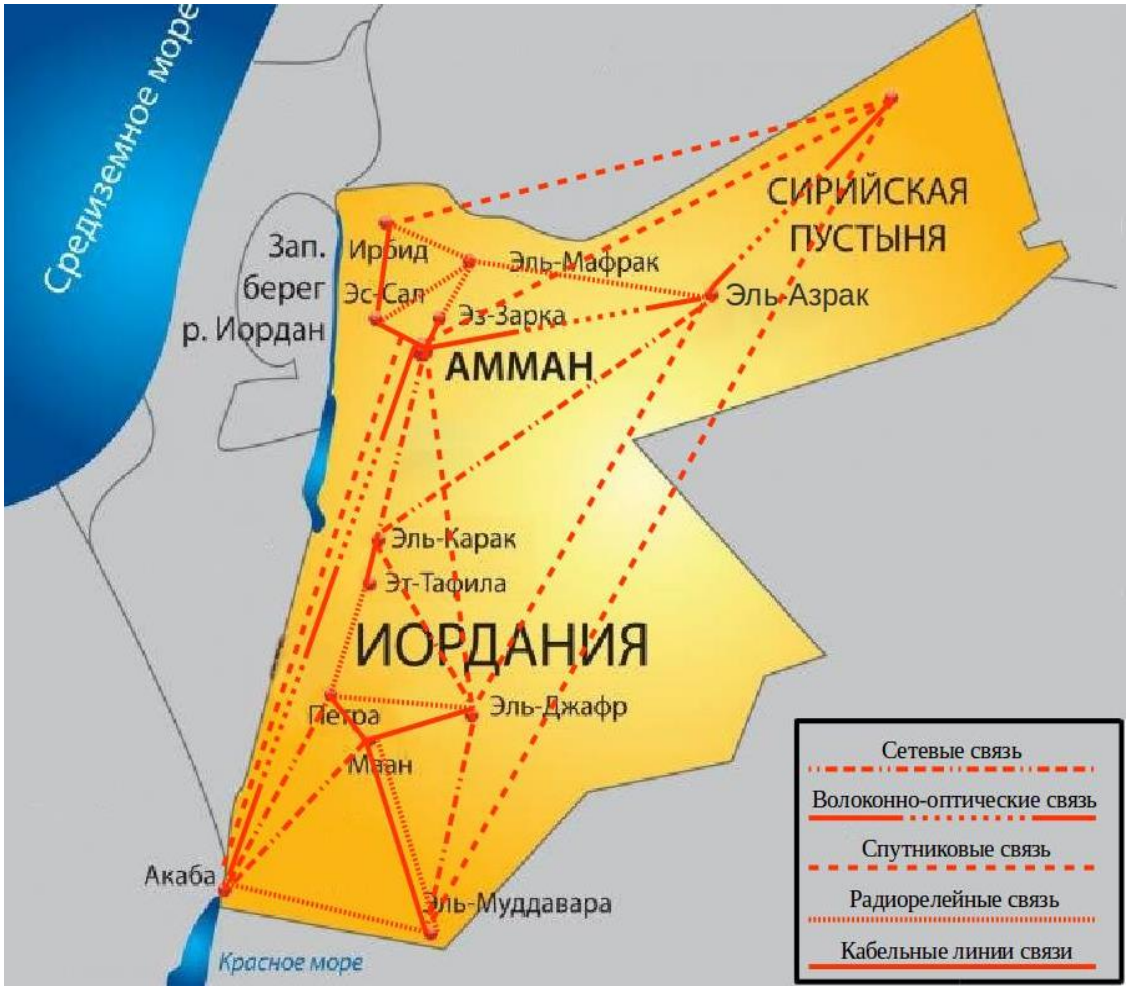


Рис.1.1.1 Карта телекоммуникационных сетей Иордании.

Радиорелейная связь: один из видов наземной радиосвязи, основанный на многократной ретрансляции радиосигналов. Радиорелейная связь осуществляется, как правило между стационарными объектами.

Исторически радиорелейная связь Иордании между станциями осуществлялась с использованием цепочки ретрансляционных станций, которые могли быть как активными, так и пассивными.

Отличительной особенностью радиорелейной связи от всех других видов наземной радиосвязи является использование узконаправленных антенн, а так же дециметровых или сантиметровых радиоволн которые используется в Иордании.

Спутниковая связь в Иордании вступила в действие в 1980 г. Станция спутниковой связи в Бакаа, приспособлена для работы с индийским спутником связи. Станция обеспечивает большой объем телефонных переговоров, передачи телексных сообщений, телевизионных программ.

С осуществлением крупного регионального телекоммуникационного проекта был положено начало использованию микроволновой связи (на 960 каналов) между Амманом и Дамаском. К системе прямой международной связи в 1982 г. были подключены Амман, Эз-Зарка, Карак, Акаба, Эль-Салт[104].

В настоящее время в сотовой связи в Иордании действует три сотовых оператора - «Заин» «Оранж» и «Умниах Umniah». Зоны их покрытия являются сплошной общей областью, и представляют набор локальных областей, разделенных между ними определенными расстояниями. Зона покрытия оператор «Заин» несколько шире, чем других.

В столице Иордании г. Амман действуют все операторы и имеют в распоряжении до 32 базовых станций каждый, образующих локальные сети. Также всех операторы действуют в достаточно крупных городах, таких, как Мадаба, Ирбид и морской порт Акаба. Локальные сети оператора «Заин » функционируют также в городах Аль-Салт, Аль-Карак и Маан. Оператор «Умниах Umniah» распределяется на крупные города иордании как Амман,

Зэрка,Ирбид,Карак. Салт,Маан и Акаба. В связи с распространением туризма, для обслуживания туристических потоков действут базовые станции «Оранж» в отдельных районах, особенно в районе пещерного монастыря «Петра» недалеко от города Маан. Оператор «Оранж » также развертывает локальные сети вдоль трасс, соединяющих Амман с Иерусалимом на западе, с Мааном и Акабой на юге и планируется развертывание вдоль трассы в восточном направлении к Ираку и на юге до границ с Саудовской Аравии.

Таким образом, несмотря на то, что уже охвачены сетями мобильной связи достаточно большое число населенных пунктов страны, остаются неохваченными значительные территория Иордании[92,113].

В Иордании произошло ухудшение качества связи вследствие более широкого использования цифрового оборудования, однако сельские районы нуждаются в лучшей телефонной связи, а в городах необходимо расширить сеть таксофонов.

Наземные спутниковые станции - 3 Интелсат, 1 Арабсат и 29 наземных и морских терминалов Инмарсат; оптоволоконный кабель до Саудовской Аравии и микроволновая радиорелейная связь с Египтом и Сирией; линия связи с международным подводным кабелем FLAG (оптоволоконный кабель, опоясывающий землю); участник Медарабтел; всего около 4 000 международных линий связи[92,104].

Волоконно-оптические линии связи: это вид связи, где информация передается по оптическим диэлектрическим волноводам, известным под названием "оптическое волокно".

Наряду со строительством глобальных сетей связи оптическое волокно широко используется при создании локальных вычислительных сетей. Оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, а также самой перспективной средой для передачи больших потоков информации на значительные расстояния, в Иордании используется волоконно-оптические линии связи

для передачи поток информации в интернете между г. Амман и г. Акаба и г. Аль-зрак и г. Амман, но их пока недостаточно.

Все каналы связи в Иордании с точки зрения защиты информации и проникновений, имеют одинаковые свойства и отличаются только скоростями и объёмам памяти, мы будем уделять внимании сетям с малоразрядным кодом и малым ёмкостями. Примерно 35% из указанных сетей используют на региональном уровне малоразрядные коды, поэтому наше рассмотрение этих вопросов актуально для Иордании[92,103,113].

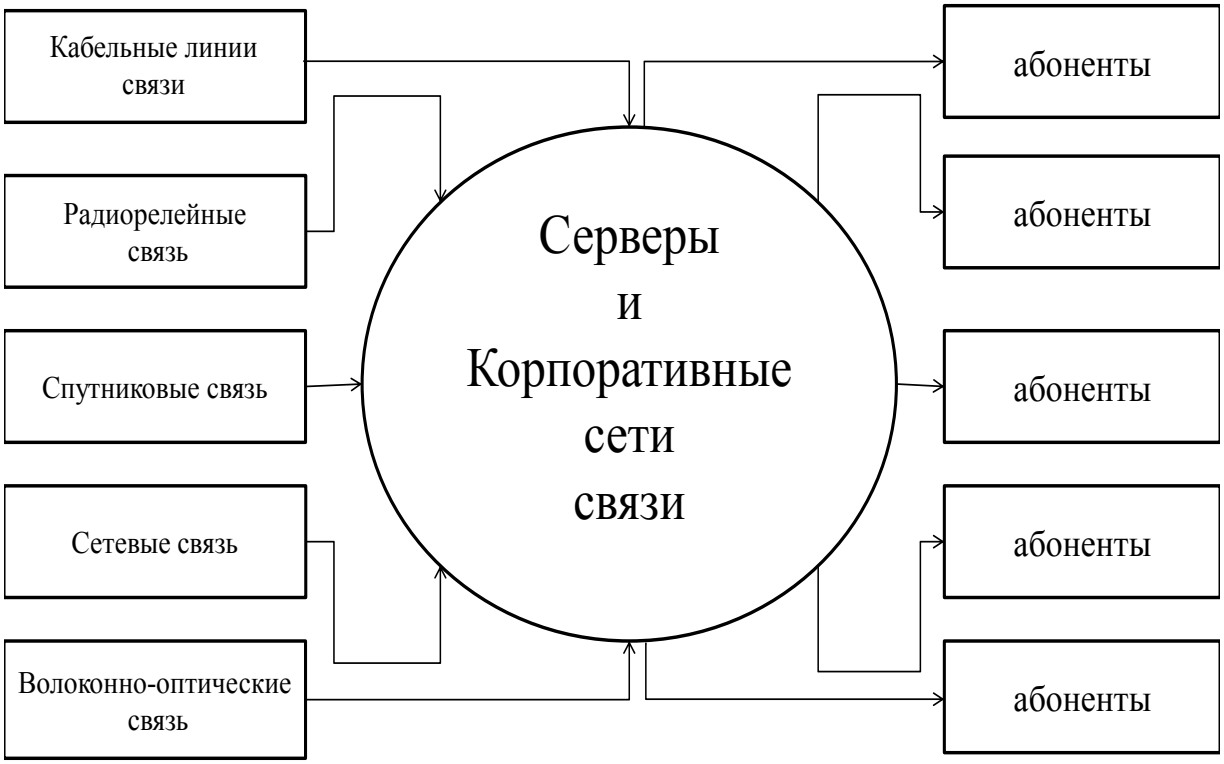


Рис 1.1.2. Структуры информационных сетей Иордании.

1.2. Анализ технических каналов корпоративных сетей по несанкционированному доступу и защите от него

Информация играет все возрастающую роль в обеспечении безопасности всех сфер жизнедеятельности общества, поэтому защита информации является одним из важных направлений деятельности в корпоративных сетях связи. Это особенно важно для Иордании, которая находится в очень близком соседстве со странами, с неустойчивыми режимами. Предприятие, которое не уделяет внимания защите от несанкционированного доступа, всегда проигрывает конкурентам, а для государства это и безопасность[1-5]. А для небольших предприятий Иордании важно еще и ограничение по затратам на это.

Основные формы информации и объекты, которым необходима защита:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, для всех форм собственности;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации ограниченного доступа, их информативные физические поля. То есть системы и средства, непосредственно обрабатывающие информацию, отнесенную к коммерческой тайне, а также конфиденциальную информацию. Эти средства и системы принято называть [4] техническими средствами приема, обработки, хранения и передачи информации (ТСПИ);
- технические средства и системы называются, которые обеспечивают действие и взаимодействие основных считают вспомогательными техническими средствами и системами (ВТСС) [4].

Перехват информации, обрабатываемой на объектах ТСПИ, осуществляется по техническим каналам.

Для приема и измерения параметров сигналов служат технические средства разведки (ТСР).

1.3. Технологическая устойчивость, конкурентная способность и информационная безопасность предприятия

Одним из критериев, определяющих финансовую устойчивость компании и конкурентную способность, являются темпы роста прибыли, опережающие темпы роста затрат на содержание компании. Поэтому на первый план выходят вопросы управления затратами и минимизации издержек. Довольно часто в этих условиях страдают ИТ-бюджеты компаний (особенно в тех организациях, где ИТ не является основным фактором производства), потому что качество и эффективность информационной системы влияют на конечные финансовые показатели опосредованно, через качество бизнес-процессов. Что касается бюджетов на защиту информации, то в этом случае, как правило, финансирование и вовсе ведется по остаточному принципу[5].

Очень важно понимать, что предприятие, которое экономит на защите, потеряет эту «экономию» в конкурентной борьбе с другими, более «разумными» предприятиями[5].

И здесь очень важно ответить на вопрос: как относиться к вложениям в информационную безопасность (ИБ) – как к затратам или как к инвестициям? Необходимо для себя разрешить противоречие: если относиться к вложениям в ИБ как к затратам, то сокращение этих затрат позволит решить тактическую задачу освобождения средств. Однако это заметно отдалит компанию от решения стратегической задачи, связанной с повышением ее адаптивности к рынку, где безопасность бизнеса в целом и ИБ в частности играет далеко не последнюю роль. Поэтому, если у компании есть долгосрочная стратегия развития, она, как правило, рассматривает вложения в ИБ как инвестиции. Именно такой подход позволяет определить цели и задачи построения системы защиты информации (СЗИ), а самое главное, он

дает возможность сосредоточиться на результатах, ожидаемых от внедрения этой системы.

В чем же разница? И затраты, и инвестиции есть отвлечение средств, необходимость потратить деньги. Разница в том, что затраты – это, в первую очередь, «осознанная необходимость», инвестиции – это перспектива окупаемости. И в этом случае требуется тщательная оценка эффективности таких инвестиций и экономическое обоснование планируемых затрат.

Основным экономическим эффектом, к которому стремится компания (а иногда и ее жизнеспособность), создавая СЗИ, является существенное уменьшение материального ущерба вследствие реализации каких-либо существующих угроз информационной безопасности. Например, по данным обзора информационной безопасности и компьютерных преступлений, подготовленного Институтом компьютерной безопасности США при участии ФБР (CSI/FBI Computer Crime and Security Survey), в 2012 году объем ущерба от утечки конфиденциальной информации среди 630 участвовавших в опросе коммерческих и государственных предприятий США составил более 370 млн. долл., ущерб от хакерских атак – более 265 млн. долл., а ущерб от вирусов – более 470 млн. долл. Здесь следует учитывать, что все участвовавшие в опросе организации обладают СЗИ [5,90,92]. Так, системы межсетевого экранирования используют 98%, системы антивирусной защиты – 99%, а системы анализа защищенности – 73%. Следовательно, можно предположить, что отсутствие этих систем защиты, а также многих других (контроля доступа, обнаружения вторжений, биометрии и т. д.) привело бы к еще более серьезным последствиям для бизнеса этих предприятий[77].

Таким образом, обеспечение информационной безопасности компании имеет вполне конкретные функциональный и экономический смыслы. А достижение этой цели должно осуществляться экономически оправданными мерами. Принимать решение о финансировании проектов по ИБ целесообразно лишь в том случае, когда вы уверены, что не просто увеличили расходную часть своего бюджета, а произвели инвестиции в

развитие компании. При этом отдача от таких инвестиций должна быть вполне прогнозируемой.

Именно поэтому в основе большинства методов оценки эффективности вложений в информационную безопасность лежит сопоставление затрат, требуемых на создание СЗИ, и ущерба, который может быть причинен компании из-за отсутствия этой системы[6,9].

Сегодня для оценки эффективности СЗИ довольно часто и наиболее плодотворно и достоверно используются такие показатели, как отдача на инвестиционный капитал (Return of Investments – ROI) и совокупная стоимость владения (Total Cost of Ownership – TCO).

ROI – это процентное отношение прибыли (или экономического эффекта) от проекта к инвестициям, необходимым для реализации этого проекта (в общем случае под инвестициями понимают TCO). При принятии решения об инвестициях полученное значение сравнивают со средним в отрасли либо выбирают проект с лучшим значением ROI из имеющихся вариантов. Несмотря на длительный опыт применения этого показателя в ИТ, на сегодняшний день достоверных методов расчета ROI не появилось, а попытки определить его путем анализа показателей деятельности компаний, внедривших у себя те или иные информационные технологии, привели к появлению показателя TCO, предложенного компанией Gartner Group еще в конце 80-х годов прошлого века. Для небольших компаний Иордании взаимодействие с проектами и между собой можно оценивать по методикам[9].

В основу общей модели расчета TCO положено разделение всех затрат на две категории: прямые и косвенные. Под косвенными затратами, как правило, понимаются скрытые расходы, которые возникают в процессе эксплуатации СЗИ.

Эти незапланированные расходы могут существенно превысить стоимость самой системы защиты. По данным той же Gartner Group, прямые

затраты составляют 15–21% от общей суммы затрат на использование ИТ[5.80.90].

1.4. Универсальные угрозы для корпоративных систем и государственных сетей Иордании

Успешные атаки на определенную информационную систему или инфраструктуру ИТ, нарушающие их функционирование, можно условно подразделить на две категории. К первой относят атаки типа «отказ в обслуживании». Ко второй — взломы, т.е. несанкционированный доступ к данным для их получения, удаления или изменения. Правда, для реализации и тех, и других атак часто используются вполне универсальные средства, имеющие «двойной» эффект — они могут и «похитить» данные, и парализовать работу предприятия. К таким средствам относятся вирусы, черви, троянцы, шпионское и рекламное ПО и т.п[32,44].

Вирусы

Наиболее старая и классическая угроза, существующая уже почти 30 лет. В настоящий момент «чистые» вирусы редко встречаются «в природе», обычно они являются составной частью более «продвинутого» вредоносного программного обеспечения (иногда по привычке называемого «вирусом») Примерами такого ПО могут быть черви и троянцы, составляющие одну из основных угроз корпоративным сетям.

Черви

По данным экспертов ежедневно обнаруживается 10-15 новых вредоносных программ. Правда, часть из них и является модификацией уже известных червей, создаваемых с целью остаться незамеченным для антивирусов в течение первых часов после начала распространения. Ситуация усугубляется еще и тем фактом, что в интернете можно найти исходные коды практически любой вредоносной программы, начиная от

бутовых вирусов-анахронизмов до самых современных червей, заражающих мобильные телефоны.

При этом если первое поколение червей распространялось в основном через электронную почту, одноранговые сети и интернет-пейджеры, то сейчас основной канал проникновения и дальнейшего распространения — дыры в программном обеспечении, число которых неуклонно растет. Ежедневно обнаруживается по 10-11 уязвимостей. Проявления этих вредоносных программ носят совершенно разный характер: от проигрыша музыкальных мелодий и синтезации речи до рассылки сообщений в чаты и демонстрации картинок фривольного содержания. Есть и более интересные варианты, например, удаление «чужих» червей. Такие «инциденты» наблюдались, например, во время войны между авторами червей Bagle и Netsky[22,31,32].

Однако есть и более серьезные последствия деятельности червей, которые наносят реальный ущерб деятельности компаний. Уже зафиксированы случаи нарушения работоспособности систем управления авиаполетами и даже электростанциями. Что же касается бизнеса, то известны случаи нарушения работы банкоматов и других корпоративных приложений. По оценкам экспертов, эпидемии вредоносных программ очень сильно мешают малому бизнесу, который не всегда имеет достаточно ресурсов для собственной защиты. В частности, в 2012 году в Западной Европе 22% малых предприятий (до 20 сотрудников) прекратили свою деятельность по причине вирусных атак, а общий ущерб от них составил 22 миллиарда евро. В Иордании пока статистика существенно спокойнее, но с развитием проектов электронного правительства она явно будет ухудшаться без принятия защитных мер[23].

Парадокс в том, что до сих пор существует непонимание всей опасности вредоносных программ. По статистике NCSA, 30% американцев уверены в том, что вероятность заражения вредоносной программой гораздо ниже, чем погибнуть от удара молнии, подвергнуться проверке налоговой

службы или выиграть миллион долларов. Однако реальность намного отличается от фантазий — ежегодно вирусным атакам подвергается 7 компьютеров из 10[85].

Троянцы

Основное отличие троянцев от червей — отсутствие механизма распространения, что, однако, не делает их менее опасными. Если черви в основной своей массе просто распространяются через интернет, нанося ущерб, в том числе и за счет захламления полосы пропускания каналов связи, то троянцы выполняют немного иную задачу — проникают на узел с целью открытия на нем скрытых каналов утечки информации. Например, троянец Mitglieder, незаметно устанавливался на компьютер-жертву и служил станцией для приема-пересылки спама. Число таких зараженных машин может измеряться тысячами, что приводит к созданию армии зомби. Другой целью внедрения может служить создание промежуточной площадки для дальнейших атак.

Троянские программы в зависимости от решаемых ими задач могут быть реализованы по-разному — от простой пересылки на указанный адрес электронной почты всей введенной пользователем информации до возможности выполнения команд, дистанционно получаемых от владельца троянца. В отдельную категорию можно выделить класс программ, которые сами по себе не являются вредоносными, но при этом облегчают установку троянцев за счет загрузки из сети интернет. Этот тип ПО тоже достаточно опасен, так как может использоваться для загрузки любой вредоносной программы, а не только отдельных версий троянских коней.

Шпионское и рекламное ПО

Очень похожим на троянцев является другой тип угроз — шпионское и рекламное ПО. Это программное обеспечение предназначено для слежения за действиями пользователя на его компьютере и пересылке собранной информации в «нечистые руки», которые могут использовать эти данные для фокусирования своей рекламы и других несанкционированных действий.

По статистике America Online (AOL), шпионское ПО установлено на 80% компьютеров пользователей. У кого-то число различных агентов-шпионов исчисляется сотнями, у кого-то «всего лишь» десятками. Со временем эксперты предсказывают этому классу угроз популярность даже большую, чем у спама.

Отдельной категорий шпионского программного обеспечения (spyware) является рекламное ПО (adware), которое является причиной ни с того, ни с сего появляющихся на экране «окошек» с надоедливой рекламой и т.д. Оно же перенаправляет ничего неподозревающих пользователей на сайты рекламодателей, рекламные площадки и другие платные ресурсы (эксперты даже выделяют отдельный тип adware — pornware, название которого говорит само за себя). Не редки случаи смены телефонного номера для коммутируемого (Dialup) соединения, что приводит к звонкам на номера, после которых на адрес пользователя приходят счета от телефонной компании на астрономические суммы.

1.5. Атаки типа «отказ в обслуживании»

DoS-атака («отказ в обслуживании») — одна из основных проблем современного Интернета. Не было еще ни одной компании, которая могла бы справиться с ней в одиночку. В качестве жертв таких атак в последние годы можно назвать Amazon, eBay, Microsoft, SCO[25,31,35].

Лавинный поток трафика сметает все на своем пути. Сервера выходят из строя, будучи не в состоянии переварить огромный поток запросов. Каналы передачи данных «забиваются» паразитным трафиком «под завязку». Процессоры инфраструктурного сетевого оборудования не успевают обработать весь идущий по сети поток данных. При этом жизнь была бы немного легче, если бы такие атаки происходили случайно или хотя бы не влекли за собой серьезного ущерба. Однако сейчас атака «отказ в обслуживании» — это просто одна из услуг, которую можно заказать в

интернете за сравнительно небольшие деньги. Стоимость такой «услуги» может составлять несколько сотен долларов, а ущерб оказывается огромным. Уже встречаются даже случаи шантажа подобными атаками. Что характерно, шантажированные платили, опасаясь серьезных потерь для своего бизнеса, а ряд несговорчивых бизнесменов действительно были атакованы подобным образом.

Подмена главной страницы сайта

Виртуальное граффити прочно прописалось в интернете. «Здесь был я» самое безобидное, что может появиться на главной странице взломанного сайта. Не нанося прямого финансового ущерба, такие действия могут повредить репутации взломанной компании, отпугнуть существующих или потенциальных клиентов и привлечь мириады других хакеров, которые попытаются повторить опыт первопроходцев. Самое интересное, что данной угрозе подвержена, абсолютна любая компания, будь то общественное движение или частное лицо.

Социальный инжиниринг

И хотя техника обмана меняется от страны к стране и должна учитывать различные культурные и национальные особенности, она является одним из основных инструментов в руках квалифицированного злоумышленника. Просьба назвать свой пароль в письме от интернет-провайдера или во время звонка от системного администратора — это типичные примеры социального инжиниринга.

Мобильная угроза

Мобильный телефон—игрушка, еще 15-20 лет назад считавшаяся уделом «избранных», теперь стала доступна любому. Такая аудитория не могла остаться незамеченной для хакерского элемента, и сейчас эксперты называют мобильные вирусы и черви одной из главных угроз будущего. Особенно учитывая всепроникающее распространение мобильных технологий по планете. Достаточно назвать только 2 примера. В феврале этого года в Санта-Монике (США) зафиксированы случаи заражения

мобильных телефонов на витрине магазина[4,8,66]. Расследование показало, что заражение произошло от обычного прохожего, шедшего мимо с инфицированным аппаратом. Учитывая какое распространение в корпоративных сетях получили в последнее время КПК, смартфоны, мобильные органайзеры, можно с уверенность говорить о том, что мобильная угроза будет одной из наиболее актуальных в XXI веке для любого предприятия.

Спам

О спаме много говорят в последнее время, принимают запретительные законы, наказывают спамеров и т.д. Однако, эта угроза неискоренима, как и неискоренима телевизионная реклама, имеющая ту же природу. Пока спам приносит организаторам немалые барыши, он будет распространяться. Да и конечному пользователю он не причиняет такого уж неудобства, как об этом постоянно твердят. Даже сотня рекламных сообщений, получаемых ежедневно, отнимает в совокупности лишь пару минут на их удаление. Хотя один из побочных эффектов спама — это либо удаление «правильных» писем с неудачной темой сообщения пользователем, или неправильно настроенные фильтры спама, которые мешают прохождению вообще всех информационных рассылок, в том числе и необходимых.

Однако есть еще одна проблема. Учитывая «военные» действия между операторами связи и авторами спаморассылок, последние никогда не совершают свои действия с личных адресов и собственных компьютеров. Обычно для этой цели используются заранее взломанные машины, на которых установлены троянские программы. Также в прайс-листе многих злоумышленников можно найти пункт об аренде сети взломанных машин для рассылки спама (это миллионы сообщений). Стоимость такой аренды — 50-100 долларов в час. И «заказать спам» тоже всего лишь одна из услуг современного Интернета, доступных в настоящий момент любому.

Фишинг

Если вы пользователь интернет-банка или интернет-магазина, есть риск стать жертвой фишинга — новой угрозы, наносящий миллиардный ущерб. Суть ее проста — вы получаете письмо, в котором ваш банк просит вас перерегистрироваться на их сайте, либо интернет-магазин уведомляет о завершении срока действия вашего пароля. Вы не подозревая, что банки так никогда не делают (они используют телефонный звонок, а не незащищенную электронную почту), заходите по ссылке любезно посланной вам банком и вводите всю нужную информацию. Однако в реальности все иначе. Вы попадаете на фальшивый сайт (в прошлом году их было более 2000), и ваши персональные данные получают злоумышленники. В прошлом году 57 миллионов человек подверглось фишинговым атакам, а среднее время жизни подставного сайта составило 6 дней. В последнее время атаки стали изощреннее — вы не просто получаете письмо со ссылкой, похожей на настоящую. В письме показывается настоящая ссылка, а сфальсифицированный адрес скрывается в коде письма. Другой пример — установка троянского коня, который переадресует все запросы на подставной сайт[54,62,83].

У злоумышленников сегодня есть огромное количество способов «вынести» всю важную конфиденциальную информацию с вашего компьютера. Каналов утечки множество:CDR,COM- и USB-порты, инфракрасный порт, Bluetooth, WiFi, встроенный модем, сетевая карта и слоты. При этом мы не учитываем монитор, кабели и т.п. с которых тоже можно удаленно считывать информацию. Если сюда добавить еще и прикладные каналы утечки информации, например, шпионское ПО, одноранговые сети, интернет-пейджеры и т.п., то можно представить, с какими сложностями сталкиваются специалисты по защите информации, вынужденные блокировать все эти пути.

Как выжить нам и нашим предприятиям (особенно малым) в этом непростом мире? Не вдаваясь в долгие обсуждения, надо отметить, что

современные методы управления непрерывным (т.е. бесконечным) процессом под названием «обеспечение информационной безопасности» позволяют использовать свое время на чтение статей о современных угрозах информационным системам, а не на поиск работы по причине банкротства предприятия, не обращавшего на них внимания.

1.6.Особенности информационной безопасности государственных сетей Иордании

Деятельность государственных сетей Иордании уже в краткосрочной перспективе будет способствовать значительному расширению использования государственных ИС для целей управления, увеличению обмена информацией и, одновременно с этим, повысит уровень информационных рисков, несанкционированной утечки, искажения, уничтожения и снижения доступности хранимой, обрабатываемой и передаваемой информации.

Существенному повышению возможности несанкционированного использования или модификации информации, блокированию процесса получения информации, введению в оборот ложной информации, приводящей к принятию ошибочных решений и, как следствие, к значительному материальному ущербу, способствуют:

- увеличение объемов обрабатываемой, передаваемой и хранимой в ИС информации;
- сосредоточение в базах данных информации различного уровня важности и конфиденциальности;
- расширение круга пользователей, имеющих доступ к государственным информационным ресурсам Иордании;
- увеличение числа удаленных рабочих мест, появление мобильных рабочих мест;

- широкое использование для связи пользователей глобальной сети Internet и различных каналов связи.

Одним из направлений государственной политики Иордании в сфере информатизации является формирование и защита информационных ресурсов государства, как национального достояния. Законы в Иордани определяет информацию как объект права[76,109,112].

Информационные ресурсы, являясь объектом отношений физических, юридических лиц и государства, подлежат обязательному учету и защите как всякое материальное имущество собственника наряду с другими ресурсами.

При этом собственнику предоставляется право самостоятельно, в пределах своей компетенции, устанавливать режим защиты информационных ресурсов и доступа к ним.

Защите подлежат только те сведения (сообщения, данные) независимо от формы их представления неправомерное обращение, с которыми может нанести ущерб гражданам Иордании, обществу или государству в целом.

Степень защиты информации определяет собственник информации, с учетом, в необходимых случаях, рекомендаций уполномоченных государственных органов. Любые нормативы на степень защиты информации, устанавливаемые регулирующими государственными органами должны базироваться на требованиях государственного законодательства.

Ответственность за выполнение мер защиты лежит не только на собственнике информации, но и на любом владельце и пользователе.

Конфиденциальной считается такая информация, доступ к которой ограничивается в соответствии с законодательством.

Законодательство Иордании содержит либо прямую норму, согласно которой какие-либо сведения относятся к категории конфиденциальных и ограничивается доступ к ним, либо определяет признаки, которым должны удовлетворять эти сведения. Законодательством определяются признаки служебной и коммерческой тайны как особого объекта гражданских прав[74,109,112].

Информационные ресурсы государственной организации и органа государственной власти также могут представлять коммерческую ценность и быть товаром, за исключением случаев, предусмотренных законодательством.

Несанкционированные действия и использование такой информации может нанести ущерб интересам не только непосредственно данной организации, но и Иордании в целом. Однако при этом, режим защиты информации, представляющей коммерческую ценность, определяется именно такой организацией или органом власти как собственником этих ресурсов[108].

Таким образом, субъектами правоотношений в процессе защиты информации при реализации функционала сетей в рамках государственных сетей Иордании [74,76]являются:

- Иордания, как собственник информационных ресурсов.
- Государственный орган или организация, уполномоченные Правительством Иордании на распоряжение переданными информационными ресурсами.
- Иные органы государственной власти, органы власти субъектов Иордании, муниципальных образований, организации, учреждения, юридические и физические лица, как совладельцы и пользователи информационных ресурсов.
- Должностные лица и сотрудники структурных подразделений учреждений, организаций, воинских формирований и подразделений, иных органов государственной власти, органов власти субъектов Иордании, муниципальных образований, организаций, учреждений, юридических лиц, а также физические лица, как пользователи информационных ресурсов.
- Юридические и физические лица, сведения о которых накапливаются в информационных ресурсах государственного органа, как собственники (владельцы) этой информации;
- Подразделения, обеспечивающие эксплуатацию технических средств обработки информации;

• Другие юридические и физические лица, причастные к созданию и функционированию технических средств обработки информации.

Объектом защиты информации в данном моменте являются сведения, содержащиеся в информационных ресурсах государственной организации, зафиксированные на материальном носителе с реквизитами, позволяющими их идентифицировать, участвующие в процессах сбора, обработки, накопления, хранения и распространения информации, доступ к которой ограничивается. Таким образом, в рамках реализации функций государственных сетей для целей оказания услуг населению основными объектами защиты могут быть:

• Информационные ресурсы органов государственной власти, региональных органов управления и муниципальных образований.

• Информационные и программные ресурсы (прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты) ИС, чувствительные по отношению к случайным и несанкционированным воздействиям, содержащие технологическую информацию управления автоматизированными системами и транспортной сетью.

• Служебные информационные ресурсы ИС (базы данных и файлы данных, системная документация, руководства пользователя) содержащие сведения о служебной, технологической и управляющей информации.

• Информационные ресурсы подсистем обеспечения безопасности информации, содержащие сведения о структуре, принципах и технических решениях защиты информации.

В перечисленных условиях обеспечение безопасности информации в системах и ресурсах государственных сетей должно быть направлено, в первую очередь, на исключение нанесения или существенное уменьшение ущерба перечисленным выше субъектам правоотношений, защиту конституционных прав личности, на сохранение личной тайны и персональных данных.

Обеспечить информационную безопасность систем государственных сетей предлагается путем создания защищенной сети передачи данных (ЗСПД) и построения подсистем обеспечения информационной безопасности (ПОИБ) для основных информационно-технических компонентов: портала государственных услуг (ПГУ); информационно-платежного шлюза (ИПШ), региональных ГС; прикладных государственных информационных систем ФОИВ. Архитектура информационной безопасности представлена на рис 1.6.1.

Рис 1.6.1. Пример схемы обеспечения информационной безопасности государственных сетей Иордании.

В ходе разработки, внедрения, эксплуатации государственных и корпоративных ИС, субъектам правоотношений может быть причинен следующий ущерб[73,116]:

1. материальный ущерб от разглашения защищаемой информации;
2. материальный, моральный ущерб от любых неправомерных действий с объектами защиты;

3. моральный, физический, материальный ущерб личности, от разглашения персональных данных;

4. моральный, материальный ущерб от нарушения конституционных прав и свобод личности;

5. материальный ущерб от необходимости восстановления нарушенных прав и объектов защиты;

6. моральный и материальный ущерб от дезорганизации деятельности;

7. материальный ущерб от уничтожения (утраты) объектов защиты и средств их обработки;

8. материальный, моральный ущерб от несвоевременного поступления информации потребителям;

9. моральный, материальный ущерб деловой репутации;

10. материальный ущерб от невозможности выполнения обязательств перед третьей стороной;

11. материальный, моральный ущерб от нарушений международных обязательств.

Примечание: 35% государственных сетей Иордания использует малоразрядные коды[113].

Таблица 1.6.1Структура защищенности государственных сетей Иордании.

Вид сети	Система безопасности	Защищенности	Использование малоразрядные коды
Мобильной	Маршрутизаторы,, кодирование,шлюзы	Защищено	используются
Проводной	Маршрутизаторы, кодирование	Защищено	используются
Радиорелейной	Кодирование	Защищено	Нет
Оптической	Маршрутизаторы, шлюзы, кодирование	Защищено	Нет

При этом причиненный ущерб может квалифицироваться как состав преступления, предусмотренный уголовным правом, или сопоставляться с рисками утраты, предусмотренными гражданским, административным или арбитражным правом.

Основными угрозами безопасности информации при разработке, создании, развитии и эксплуатации государственных ИС Иордании являются:

- для нарушения конфиденциальности информации:
- хищение (копирование) информации и средств ее обработки
- утрата (неумышленная потеря, утечка) информации, средств ее обработки
- для нарушения целостности информации:
- модификация (искажение) информации
- отрицание подлинности информации
- навязывание ложной информации
- для нарушения доступности информации:
- блокирование информации
- уничтожение информации и средств ее обработки

Для достижения целей защиты и нейтрализации угроз информационной безопасности при осуществлении деятельности государственных сетей Иордании должно быть обеспечено эффективное решение задач:

1. защита от вмешательства в процесс функционирования государственных ИС со стороны пользователей, иных неуполномоченных и посторонних лиц, в том числе легальных пользователей этих ресурсов;
2. обеспечение полноты, достоверности и целостности сведений, содержащихся и вносимых в указанные ИС;

3. обеспечение физической сохранности технических средств и программного обеспечения ИС и защита их от действия техногенных и стихийных источников угроз;

4. регистрация событий, влияющих на безопасность информации, обеспечения полной подконтрольности и подотчетности выполнения всех операций, которые могут оказать влияние на состояние информационной безопасности ИС и циркулирующей в них информации;

5. своевременное выявление, оценка и прогнозирование источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба интересам субъектов правоотношений, нарушению нормального функционирования и развития государственных ИС;

6. анализ рисков реализации угроз безопасности информации и оценка возможного ущерба, предотвращение неприемлемых последствий нарушения безопасности информации, циркулирующей в ИС, создание условий для минимизации и локализации наносимого ущерба;

7. обеспечение возможности восстановления актуального состояния ИС при нарушении безопасности информации и ликвидации последствий этих нарушений;

8. формирование целенаправленной политики в области обеспечения безопасности информации при разработке, внедрении, эксплуатации и совершенствовании ИС.

Основные принципы обеспечения безопасности информации в государственных информационных системах, вовлеченных или связанных с деятельностью государственных сетей[74,104,112].

- Принцип законности. Проведение защитных мероприятий должно быть согласовано с действующим законодательством в области информации, информатизации и защиты информации с применением всех дозволенных методов обнаружения и пресечения нарушений при работе с информацией.

- Принцип максимальной дружественности и прозрачности. Противодействие угрозам безопасности информации всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу ИС, так как меры по защите информации всегда налагают ограничения на работу организационного и технического характера. Поэтому принимаемые меры должны максимально совмещаться с используемыми операционной и программно-аппаратной структурой ИС, а также должны быть понятны и оправданы для пользователей.

- Принцип превентивности. Меры по защите информации и внедряемые СЗИ должны быть нацелены, прежде всего, на недопущение (пресечение) реализации угроз безопасности информации, а не на устранение последствий их проявления.

- Принцип оптимальности и разумной разнородности. Для сокращения расходов на создание систем обеспечения безопасности должен осуществляться оптимальный выбор соотношения между различными методами и способами противодействия угрозам безопасности информации. Дополнительно внедряемые средства защиты должны дублировать основные функции защиты, уже используемые в программно-аппаратной среде ИС, и по возможности иметь другое происхождение, чем сама эта среда, что позволяет существенно затруднить процесс преодоления защиты за счет иной логики построения защиты.

- Принцип адекватности и непрерывности. Решения, реализуемые системами защиты информации, должны быть дифференцированы в зависимости от важности защищаемой информации и вероятности возникновения угроз ее безопасности. Безопасность информации в государственных информационных системах должна обеспечиваться непрерывно в течение всего жизненного цикла систем.

- Принцип адаптивности. Системы обеспечения информационной безопасности должны строиться с учетом возможного изменения

конфигурации ИС, роста числа пользователей, изменения степени конфиденциальности и ценности информации.

- Принцип доказательности и обязательности контроля. Должны реализовываться организационные меры внутри сети и применение специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации. Должна обеспечивать обязательность, своевременность и документированность выявления, сигнализации и пресечения попыток нарушения установленных правил защиты.

- Принцип самозащиты и конфиденциальности самой системы защиты информации.

- Принцип многоуровневости и равнопрочности. ИС должна реализовывать защиту информации на всех уровнях своей жизнедеятельности (технологическом, пользовательском, локальном, сетевом). Защита должна строиться эшелонировано, и иметь несколько последовательных рубежей таким образом, чтобы наиболее важная зона безопасности находилась внутри других зон. Все рубежи защиты должны быть равнопрочными к возможности реализации угрозы.

- Принцип простоты применения и апробированности защиты. Должны применяться средства защиты, для которых формально или неформально возможно доказать корректность выполнения защитных функций, проверить согласованность конфигурации различных компонентов, а их применение пользователями и обслуживающим персоналом должно быть максимально простым, чтобы уменьшить риски, связанные с нарушениям правил их использования. По той же причине целесообразно использовать средства защиты информация допускающие возможность централизованного администрирования.

- Принцип преемственности и совершенствования. Система защиты информации должна постоянно совершенствоваться на основе

преемственности принятых ранее решений и анализа функционирования ИС.

- Принцип персональной ответственности и минимизации привилегий для пользователей всех уровней. Принимаемые меры должны определять права и ответственности каждого уполномоченного лица. Распределение прав и ответственности должно в случае любого нарушения позволять определить круг виновных. Система обеспечения информационной безопасности должна обеспечивать разделение прав и ответственности между пользователями.
- Принцип персональной ответственности и минимизации привилегий для пользователей всех уровней. Система обеспечения информационной безопасности должна обеспечивать разделение прав и ответственности между пользователями и минимизацию привилегий, позволяя, в случае любого нарушения, определить круг виновных.

Эти особенности рассмотрены нами в [98,99,100].

Программно-аппаратная инфраструктура ключевых систем государственных сетей Иордании.

Единого портала госуслуг (ЕПГУ) и Системы межведомственного электронного взаимодействия (СМЭВ).

В 2012 г. для ЕПГУ было приобретено более 5 серверов HP, несколько маршрутизаторов Cisco и систем хранения Hitachi вместе с СУБД Oracle. Для СМЭВ использовались один блейд-сервера и ленточная библиотека Sun, сервер HP, дисковый массив Hitachi и коммутатор Brocade. В качестве программной шины было приобретено решение Oracle.

Предположим в 2016 г. вычислительные мощности расширяется. На этот раз в основном за счет оборудования IBM. Инфраструктура ЕПГУ потребляет 8 новых серверов, СМЭВ — три. Помимо этого, техника IBM с 2016 г[71,107].

1.7. Оценка эффективности информационного канала с учётом защитных мероприятий

Рассмотрим возможные критерии, которые на наш взгляд полностью подходят для решение задач защита информации государственных сетей Иордании. Известно, что наиболее удобные и достоверные критерии эффективности (Э) для этого те, в которых использованы: риски, потери от проникновений, штрафы, затраты на ЗМ (З), приведенные затраты (П) и другие, часто, экономические параметры. Рассмотрим их [9,117].

$$\max Эм = \frac{П_{\Sigma}}{З_{с} + З_{экс}} \qquad (1.7.1)$$

$$\max \left\{ П_{\Sigma} \right\} \Big/ (З_{с} + З_{экс}) \le З_{с} \qquad (1.7.2)$$

$$\frac{\min\{Зс + Зэкс\}}{П_{\Sigma}} \le Пзад \qquad (1.7.3)$$

$$\frac{\max\{П_{\Sigma}\}}{\min\{Зс + Зэкс\}} \qquad (1.7.4)$$

Наиболее объективная форма – (4), → количественная форма – (1).

Упрощение приводит к (2) или (3). Для спецприменений может быть предпочтительно (2). Поскольку явно или неявно проектировщик, пользуясь (1), проверяет (2) или (3), то недостатки (1), могут привести к нечеткому решению, существенно компенсируются.

Эффективность моделирования имеет существенное значение в процессе эффективности оценки, эффективности проектирования. Трудности определения эффективности моделирования (ЭМ) в условиях взаимозависимых связей. ЭМ необходимо оценивать в случаях выбора

варианта модели телекоммуникаций (которые чаще всего в основном-радиосистемы (РТС) с целью улучшения эффективности проектирования (ЭПр) при предположении несанкционированного проникновения.

В данном подходе под ЭМ понимается комплексный критерий качества модели.

Требования к показателю качества модели:

- определять в какой степени модель позволяет достигнуть поставленной цели;
- быть количественным, чтобы сравнение моделей было обоснованным;
- допускать достаточно простую физическую трактовку;
- быть статистически устойчивым, т.е. иметь малый разброс относительно среднего значения.

Чаще всего при оценке ЭМ (когда этот вопрос поднимается) понимают только адекватность, забывая о том, что затраты на различные варианты моделей могут быть существенно различными.

Для большей объективности целесообразно оценивать ЭМ интегральным критерием:

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

где Π_{Σ} – суммарный полезный эффект;

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

Часто при проектировании трудно конкретно (количественно) оценить Π_{Σ}. Тогда целесообразно применение индексной формы интегрального критерия.

В инженерной практике могут найти применение следующие разновидности, удовлетворяющие указанным условиям:

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

Где q_i – относительный критерий, например вида:

$$q_i = \frac{p_i}{p_{iб}}$$

или показатель адекватности (точности соответствия) по какому-либо параметру (характеристики)

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.

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

Такой подход возможен при моделировании различных видов систем и их характеристик (линейным и нелинейным, стационарным и нестационарным, дискретным и непрерывным, с одним или несколькими входными воздействиями, детерминированных и стохастических процессов) поэтому, что все это учитывается в показателе q_i. При применении базовых показателей эти трудности значительно уменьшаются.

Индексные показатели можно распространить для оценки общей эффективности нескольких моделей или для оценки общей эффективности нескольких процессов проектирования[35].

$$Э_{\Sigma} = \frac{\sum_{j=1}^{l} C_j Э_{мj}}{\sum_{j=1}^{l} C_j}.$$

Такие формы критериев можно использовать в инженерных оптимизациях (субоптимизациях и парциальных оптимизациях).

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

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

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

Таблица 1.7.1.Пример расчета для структуры (рис 1.6.1).

№	q1	q2	q3	C1	C2	C3
1	0, 1	0, 7	0, 9	5	3	2
2	0, 4	0, 5	0, 6	4	5	3
3	0, 2	0, 1	0, 3	2	3	2

$$Ик1 = \frac{0,1*5 + 0,7*3 + 0,9*2}{5+3+2} = \frac{4,4}{10} = 0,44,$$

$$Ик2 = \frac{0,4*4 + 0,5*5 + 0,6*3}{4+5+3} = \frac{5,7}{12} = 0,48,$$

$$Ик3 = \frac{0,2*2 + 0,1*3 + 0,3*2}{2+3+2} = \frac{1,3}{7} = 0,18.$$

Эффективность оценивается в случаях выявления целесообразности моделирования и в случаях сравнения различных моделей. При первом затраты инвариантны, при втором – необходимы интегральные критерии с каким-либо количественным выражением затрат в знаменателе. При первом критерии: эквивалентный эффект, время проектирования, качество проектирования и т.п. При втором в числителе: точность по группе параметров, адекватность в каком-либо смысле, какой-либо критерий эффективности от моделирования; в знаменателе: время и другие ресурсы, например, адекватность, точность, статистическая адекватность.

Возможно будет важнее не адекватность (точность соответствия) по одному или группе параметров, а затраты на моделирование (время, средства и т.п.)

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

Такой подход возможен к различным видам систем и их характеристикам (линейным и нелинейным, стационарным и нестационарным, дискретным и непрерывным, с одним или несколькими входными воздействиями, детерминированных или стохастических процессов). Описание действующей системы, когда ее структура неизвестна, формируется с помощью ее идентификации, т.е. подбора аппроксимирующих соотношений с той или иной полнотой отображающих поведение наблюдаемой системы [9, 117].

$$Эм = \frac{П_{\Sigma}}{Зс + Зэкс},\ q_i = \frac{P_i}{P_{bi}},$$

$$Эм = \frac{\sum_{i=1}^{S} n_i q_i L_i}{\sum_{i=1}^{S} n_i L_i} \quad ; \tag{1.7.5}$$

$$Эм = \frac{\sum_{i=1}^{S} q_i C_i}{C};\ C_i = n_i L_i;\ C = \sum_{i=1}^{S} n_i L_i = \sum_{i=1}^{S} C_i\ ; \tag{1.7.6}$$

$$Эм = \frac{\sum_{i=1}^{S} \alpha_i q_i C_i}{\sum_{i=1}^{S} C_i};\ \sum_{i=1}^{S} \alpha_i = 1; \tag{1.7.7}$$

$$Эм = \frac{\sum_{j=1}^{l} C_j Эмj}{\sum_{j=1}^{l} C_j}\ ; \tag{1.7.8}$$

При исследовании РТС и методом математического моделирования на ПК применяются все способы описания: обобщенное, детальное и идентификация.

Математическая модель системы, таким образом, - упрощенное и формализованное ее описание. Показатель качества должен[117]:

- определить, в какой степени система позволяет достигнуть поставленной цели;
- быть количественным, чтобы сравнение системы было обоснованным;
- допускать достаточно простую физическую трактовку;
- быть статистически устойчивым, т.е. иметь малый разброс относительно среднего значения.

1.8. Выводы по главе 1

1.Обосновано, что обеспечение защиты информации имеет громадное значение для повышения конкурентоспособности предприятий и сохранения его технологической деятельности. При этом для небольших предприятий Иордании при взаимодействиях в рамках государственных сетей между собой важно соблюсти разумные затраты.

2.Существует проблема внедрения современных технологий на устаревшем оборудовании с малыми емкостями и скоростями, поэтому лучше использовать малоразрядные коды и защиту маршрутизаторов в сетях от различных проникновений.

3.Доказывается необходимость выявления несанкционированных проникновений в сети и каналы предприятий и целесообразного обеспечения защиты.

4.Рассмотрены различные пути обеспечения информационной защиты предприятий и выигрыш от их внедрения.

5.Предложено обеспечить информационную безопасность систем государственных сетей Иордании путем создания защищенной сети передачи данных (ЗСПД) и построения подсистем обеспечения информационной безопасности (ПОИБ) для основных информационно-технических компонентов государственных сетей Иордании.

6.Приведены пригодные для особенностей Иордании оценки эффективности защищенных корпоративных телекоммуникационных сетей.

ГЛАВА 2. МЕТОДИКИ ДЛЯ РАСЧЁТОВ ЦЕЛЕСООБРАЗНОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Как отмечалось, для каждого типа угроз может быть одна или несколько мер противодействия.

В зависимости от уровня конкурентоспособности предприятий необходимы различные затраты на информационную безопасность. Они должны быть обоснованны.

В связи с неоднозначностью выбора мер противодействия необходим поиск некоторых критериев, в качестве которых могут быть использованы надежность обеспечения сохранности информации и стоимость реализации защиты. Принимаемая мера противодействия с экономической точки зрения будет приемлема, если эффективность защиты с ее помощью, выраженная через снижение вероятного экономического ущерба, превышает затраты на ее реализацию. В этой ситуации можно определить максимально допустимые уровни риска в обеспечении сохранности информации и выбрать на этой основе одну или несколько экономически обоснованных мер противодействия, позволяющих снизить общий риск до такой степени, чтобы его величина была ниже максимально допустимого уровня. 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 рассматривает любой механизм аппаратной защиты как некоторые дополнительные затраты с

желанием за их счет снизить общие расходы. При решении на уровне руководителя проекта вопроса о разработке аппаратных средств защиты необходимо учитывать соотношение затрат на реализацию процедуры и достигаемого уровня обеспечения сохранности информации. Поэтому разработчику нужна некоторая формула, связывающая уровень защиты и затраты на ее реализацию, которая позволяла бы определить затраты на разработку потребных аппаратных средств, необходимых для создания заранее определенного уровня защиты. В общем виде такую зависимость задают исходя из следующих соображений. Если определять накладные расходы, связанные с защитой, как отношение количества использования некоторого ресурса механизмом управления доступом к общему количеству использования этого ресурса, то экономические методы управления доступом дадут накладные расходы, приближающиеся к нулю.

2.1. Оценка эффективности мероприятий по защите корпоративных сетей Иордании от несанкционированного доступа

Ранее мы отметили, что наиболее достоверные критерии эффективности при защите от НСД – технико-экономические. При оценке необходимости защиты предприятия от несанкционированного доступа к информации можно считать, что полные затраты (потери) определятся выражением, которое нужно минимизировать, мы используем методику [9,117] для оценки эффективности корпоративных сетей Иордании.

$$Rзатр = rпот\ Рпи\ Рнпи + rмер\ Ропи\ Роопи \rightarrow \min,$$

где полные потери

rпот = Rнез.сд. + R сорв.сд.;

Rнез.сд.--прибыль от незаключенных договоров;

Rсорв.сд. - прибыль от сорванных договоров;

стоимость затрат на информационную защиту

Rмер. = Rапп. +Rэкс. + Rреж ;

Rапп. - затраты на аппаратуру;

Rэкс. - эксплуатационные затраты;

R реж. - затраты на организацию режима на предприятии;

Рпи - вероятность потерь информации;

Рнпи - условная вероятность необнаружения потерь информации;

Ропи = (1-Рнпи) - вероятность отсутствия потерь информации,

(так как они составляют полную группу событий),

Роопи - условная вероятность ошибки в обнаружении потерь информации.

При этом надо учитывать, что

Рнпи $\rightarrow$ 1

при отсутствии аппаратных средств контроля, а

Рооп $\rightarrow$ 0

при полном охвате контролем.

Учитывая необходимость минимизации выражения полных потерь, целесообразность использования защиты будет при соблюдении условия Rпот Рпи Рнпи > rмер.Ропи Роопи.

Практически это можно определить по формуле

Rпот.Рпи Рнпи =krмер.(1-Рпи)Роопи . [9,117].

При этом k=(2-5) и он выбирается больше при большем вложении в это предприятие (страховочный подход). [9,117].

Козффициент назначается заказчиком, исходя из своих условий и потребностей.

Вероятность не обнаружения потерь информации

$$Рнпи = 1 - \sum_{i=1}^{N} Pi.$$

Учитывая определенный опыт нескольких предприятий, можно считать[9,66]:

Р1 =0,1 - при установке аппаратуры по защите от подслушивания в помещении;

Р2 =0,1-0,2 - при установке аппаратуры по защите от подслушивания по телефону;

Р3 =0,1-0,2- при проведении мероприятий по защите компьютерных сетей;

Р4 =0,1 - при введении на предприятии режима;

Р5 =0,1 -при защите от записи на диктофон.

Несмотря на другой (с точки зрения знака и природы) характер зависимости вероятность ошибки в обнаружении потерь информации можно приближенно определить как

$$Роопи = 1 - \sum_{i=1}^{N} Pi \ .$$

Такой подход в оценке необходимости защиты информации безусловно правомерен на предварительном этапе решения, поскольку не требует большого количества статистических данных.

Эти методики апробированы на конкретных предприятиях (см. Приложение 5,6,7) и показали хорошие результаты.

2.2.Зависимость эффективности корпоративной сети связи Иордании от срывов

Постановка задачи. Необходимость.

Эффективность систем радиосвязи зависит, в частности, от количества и длительности срывов связи между различными абонентами и центрами[44,45,46,66,117].

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

Рассматриваемая сеть 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,

$$\sum_{l=0}^{n} K_l = n_{ji} \qquad (2.2.1)$$

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;
- где n – максимальное число абонентов в канале.

Для такой системы выполняется равенство:

$$K_0 + \sum_{l=1}^{n} K_l \, l = N\text{-}1 \qquad (2.2.2)$$

Оценивать надежность такой системы можно, допуская ординарность любого потока событий в ней и отсутствие последствия, что чаще всего соблюдается на практике. Это позволяет считать, что средняя частота срывов связи λ и средняя длительность времени срыва $\Delta t_{ср}$ для всех элементов – Марковский процесс.

Расчетные соотношения.

Рассмотрим канал как систему, состоящую из l элементов, в любом из которых может наступить срыв или восстановление связи. Пусть вероятности $P_0(t)$, $P_1(t)$,…, $P_k(t)$, $P_l(t)$ соответствуют тому, что в данный момент времени в системе (канале), соответственно, нет срывов, один срыв, два срыва связи и т.д. Причем для любого момента времени

$$\sum_{k=1}^{l} P_k(t) = 1 \qquad (2.2.3)$$

Решение системы уравнений Эрланга (1) для этого случая позволяет найти вероятность наступления k срывов связи в канале. Если рассматривать стационарный режим работы сети, то все производные $P'_h(t)$ и для $P_h(t)$ получим

$$P_k(t) = \frac{\lambda^k}{k!\,\mu k} P_o(t) \qquad (2.2.4)$$

Где - $\mu = \Delta t_{cp}$

Отношение $\lambda/\mu=\alpha$ имеет физический смысл приведенной плотности наступления срывов. Очевидно, что сеть работоспособна, если $\alpha<1$.

$$P_0(t)\sum_{k=0}^{1}\frac{\alpha^k}{k!}=1$$

Используя условие (2.2.4), получим:

Откуда:

$$P_0(t) = 1\Big/\sum_{k=0}^{1}\frac{\alpha^k}{k!}$$

$$P_k(t) = \frac{\alpha^k}{k!\sum_{k=0}^{1}(\alpha^k/k!)} \qquad (2.2.5)$$

Выражение для $P_k(t)$ получены в предположении, что частоты срывов и восстановления связи подчиняются показательному закону. Однако, как следует из эргодической теории, следует неизменность формул Эрланга при любом распределении времени событий в системе, но конечном и постоянном значении его математического ожидания[66]. Это позволяет значительно расширить область применения формул Эрланга для решения многих практических задач, не производя критериальных оценок законов распределения[38,43].

Считаем, что связь по данному каналу нарушается, если происходит срыв хотя бы у одного из абонентов в канале. Вероятность того, что внутри канала хотя бы в одном звене произойдет срыв, равна:

$$P_1 = \frac{\alpha}{\sum_{k=0}^{l} (\alpha^k / k!)} \qquad (2.2.6)$$

Относительная надежность канала задается как:

$Y^k_{ij} = 1 - \Delta t^k_{ij}/t^k_{ij}$, где Δt^k_{ij} – время срыва связи между i – м и j – м абонентами по k – тому каналу связи; t^k_{ij} – полное время работы k – того канала. При больших временах работы отношение $\Delta t^k_{ij}/t^k_{ij}$ будет стремиться к вероятности срыва связи в канале, т.е. к величине P1, определяемой соотношением (6), и относительная надежность работы канала связи между i – м и j – м

$$y^k_{ij} = 1 - P_1 = 1 - \alpha / [1 + \alpha + \sum_{k=2}^{l} (\alpha^k / k!)] \qquad (2.2.7)$$

абонентами может быть выражена:

Если $\alpha << 1$ (практически $\alpha \leq 0{,}1$) и l – конечно, то выражения (2.2.6)

и (2.2.7)

значительно упростятся:

$P1 \approx \alpha / (1 + \alpha)$;

$Y^k_{ij} \approx 1 - \alpha / (1 + \alpha) = 1 / (1 + \alpha)$.

Относительная надежность связи между i – м и j – м абонентами по всем n_{ij} каналам определяется из соотношения:

$y_{\sum ij} = 1 - \Delta t_{\sum ij} / t_{\sum ij}$

При больших временах работы $\Delta t_{\sum ij} / t_{\sum ij}$ стремится к $P_{\sum ij}$ – результирующей вероятности полного срыва связи между i – м и j – м абонентами по всем n_{ij} каналам связи. Поскольку срывы связи в разных каналах можно считать независимыми, то вероятность срыва по всем

каналам будет равна произведению вероятностей срыва отдельных каналов (P1),

Т.е.:

$P_{\sum ij} \approx P_1^{n}{}_{ij}$ и

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

При условии $\alpha << 1$ и, конечно же, n_{ij}, $P_{\sum ij} = \alpha^{nij}/(1+\alpha)^{nij}$, а

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

рассматривая надежность связи между абонентами i и всеми j – ми по возможным N_{ij} каналам связи, имеем аналогично предыдущему

$y_{\sum i} = 1 - \Delta t_{\sum i}/t_{\sum i}$, где $\Delta t_{\sum i}/t_{\sum i} \rightarrow P_{\sum i}$ – вероятность срыва связи между i – м и всеми j – ми абонентами по всем N_{ij} каналам.

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

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

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

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

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

Полагая N достаточно большим ($N > 10$ и $\alpha << 1$), получаем:

Итоговые соотношения

Окончательно для определения зависимостей между:

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

y^k_{ij}, $y_{\sum ij}$ и $y_{\sum i}$, получаем соотношения[117]:

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

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

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

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

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

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

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

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

$(1 - y_{\sum i})^{1/Nij} = (1 - y)^{1/N} = (1 - y_{\sum ij})^{1/nij}$; (3.2.8)

Значениям y можно придавать смысл уровня технического состояния сети Иордании (или соответствующей ее части) [5,8,66,93] и использовать при выборе вариантов проектирования или оценке качества работы сети Иордании.

2.3. Оценка эффективности информационного канала с учетом защитных мероприятий

Чаще всего в случае применения защитных мероприятий (ЗМ) в канале (как правило, радиоэлектронной системе (РЭС) и аппаратуры корпоративных сетей Иордании выигрыш получается за счет уменьшения расходов на эксплуатационные потери, при этом, очевидно что, $П_{изн} > П_{изс}$ по причине повышения качества (улучшения параметров , точности, надежности и т .д.).

Тогда приведенные затраты получаются из соотношения [66,117]

$$П_э = \varepsilon + E(П_{из} + К_м + \ldots) . \qquad (2.3.1)$$

Здесь $К_м$ - расходы на монтаж и установку РЭС.

В расходы по эксплуатации ε обязательно вводятся составляющие , которые зависят от качества РЭС

$$\varepsilon = C_э + C_р + C_{пр} + C_г + C_{кач} , \qquad (2.3.2)$$

где $C_э$ - эксплуатационные расходы на энергию, зарплату обычному личному составу и т.д.;

$C_р$ - расходы на ремонт с учетом замененных деталей и зарплаты личному составу повышенной квалификации;

$C_{пр}$ - расходы из-за временной неработоспособности (простоя) РЭС, которые отрицательно отражаются на обслуживаемых процессах;

$C_г$ - стоимость потери какой – либо обслуживаемой технической системы или нарушения технологического процесса из-за отказа РЭС или проникновения в нее;

$C_{кач}$ - составляющая, зависящая от качества РЭС, а именно от одного или ряда определяющих параметров самолета. В эту же составляющую включаются стоимость тех мероприятий, которые произвели в обслуживаемом комплексе, в связи с улучшением качества РЭС (защитили канал).

Очевидно, чем выше качество новой РЭС, тем меньше величина $C_{кач}$ в соотношении (2.3.2).

Необходимо отметить, что перечисленные составляющие являются функциями в первом приближении от небольшого числа параметров РЭС [66].

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

Здесь θ- время эксплуатации;

S - величина, зависящая от сложности РЭС и аппаратуры корпоративных сетей ;

G - величина, определяемая энергетическими показателями РЭС ;

H - величина,определяемая одной или совокупностью характеристик надежности РЭС и аппаратуры корпоративных сетей;

V - обьем обслуживания какой – либо технической системы с помощью РЭС (часть информационной продукции);

M - стоимость материальных ценностей ,обслуживаемых РЭС;

P - значения определяющих параметров;

Z - изменение стоимости других систем при внедрении новой РЭС и аппаратуры корпоративных сетей (с защитными мероприятиями).

Перечисленные составляющие являются вполне определенными для конкретных РЭС и аппаратуры корпоративных сетей (это показано ниже, на примере).

После нахождения всех составляющих (2.3.1) и (2.3.2), можно определить эффективность контроль.

Приведенные затраты на эксплуатацию сетевых РЭС и аппаратуры корпоративных сетей с ЗМ определяются соотношением

$$П_{э\ РЭС\text{-}ЗМ} = \varepsilon_{РЭС\text{-}ЗМ} + E\ (\ П_{ИЗРЭС} + П_{ИЗКУ} + К_{МРЭС} + К_{МЗМ} + \ldots)\ , \quad (2.3.3)$$

и

$$\varepsilon_{РЭС\text{-}ЗМ} = c_{ЭРЭС} + c_{ЭЗМ} + c'_{Р} + c'_{ПР} + c'_{Г} + c'_{КАЧ}\ . \quad (2.3.4)\ .$$

Эффективность внедрения ЗМ в одном комплексе определиться как

$$Э = П_{э\ РЭС} - П_{э\ РЭС\text{-}ЗМ} = - c_{ЭЗМ} + (c'_{Р} - c'_{Р}) + (c_{ПР} - c'_{ПР}) + (c_{КАЧ} - c'_{КАЧ}) + E(\ -П_{ИЗЗМ} - К_{МЗМ}). \quad (2.3.5)$$

Здесь значения со штрихами – соответствующие расходы после внедрения ЗМ.

Очевидно, чем более глубокий и всесторонний контроль, тем меньше (по абсолютной величине) $c'_{Р}$, $c'_{ПР}$, $c'_{Г}$ и $c'_{КАЧ}$, но в то же время возрастают $c_{ЭЗМ}$, $П_{ИЗЗМ}$, $К_{МЗМ}$.

Следовательно , необходимо выбирать целесообразный вариант ЗМ с точки зрения получения наибольшей экономической эффективности .

Часто бывают трудности при определении $С_{ПР}$ и $С_{Г}$.

Когда еще нет достаточных статистических данных. В этом случае целесообразно, как это показано ранее[66,117] приближенно оценивать их соотношениями

$С_{ПР} \supseteq \theta k(Н)(c_{Э} + c_{Р})2$;

$С_{Г} \supseteq k(Н)С_{ТЕХН.КОМПЛЕКСА}$,

где k(Н) -коэффициент, характеризующий надежность сетевых РЭС и аппаратуры корпоративных сетей.

Чаще всего $k(Н) = 1-К_{Г}$

Или $k(Н) = 1- Р_{нф}$

Здесь $Р_{нф}$ - вероятность нормального функционирования РЭС и аппаратуры корпоративных сетей

Выбор соотношений основан на следующих простых предположениях:

-необходимость непрерывной работы технической системы или информационных средств, в составе которой находиться РЭС и аппаратуры корпоративных сетей;

-для исключения аварий или проникновений, как правило, создают какой – либо дублирующий комплекс.

К сожалению, для многих систем определение перечисленных составляющих является достаточно сложным и часто приближенным.

Иногда возникает задача оценки эффективности при отсутствии прототипа.

В этом случае необходимо оценить какие высвободились материальные ресурсы в связи с применением РЭС и аппаратуры корпоративных сетей[38,46].

Предполагается, что эта операция проводилась ранее каким – то другим способом. Или же берется ближайший вариант выполнения тех же функций (того же эффекта) и определяется эффективность относительно него.

В случае заданных средств определяется, сколько нужных систем с определенным качеством можно создать на эти средства.

Попробуем количественно связать значение стоимости с показателями надёжности (один из критериев показателей качества).

Общая стоимость РЭС за время эксплуатации θ

$$C = C_к + C_э + C_р + C_{пр} + C_г \quad , \qquad (2.3.6)$$

где $C_к$ - первоначальная стоимость (приведённые затраты на изготовление, монтаж и т.д. с обычным учётом нормативного коэффициента Е) .

Все остальные аналогичны по смыслу обозначениям из соотношения (2.3.2) .

Первоначальную стоимость можно связать с надёжностью при помощи математической модели

$$C_к = A /(1-P^a)^b \quad , \qquad (2.3.7)$$

где A, a, b – коэффициенты, зависящие от вида аппаратуры, её назначения, условий эксплуатации и т.д.;

P – вероятность безотказной работы РЭС и аппаратуры корпоративных сетей.

Для восстанавливаемой РЭС и аппаратуры корпоративных сетей более оправдано, на наш взгляд, применение вместо Р коэффициента готовности $К_Г$ или вероятности нормального функционирования.

Эксплуатационные расходы $C_Э$ мало зависят от требуемой надёжности, поэтому для упрощения эту составляющую можно не учитывать.

Расходы на ремонты (последствия ненадёжности РЭС и аппаратуры корпоративных сетей)

$$СР = \theta\, \tau_b\, Сраб / T_0 + \alpha\, Ск\, \theta\, \beta / T_0 N , \qquad (2.3.8)$$

где θ / T_0 - среднее число отказов за время θ (число восстановлений);

τ_b – среднее время одного восстановления (ремонта) – обычно в часах;

Сраб – зарплата обслуживающего персонала повышенной квалификации за единицу времени;

α Ск / N – средняя стоимость одной заменённой детали (N – условное число деталей РЭС и аппаратуры корпоративных сетей, приведённое к средней стоимости заменяемых деталей, α- коэффициент, учитывающий условия хранения и комплектацию); аналогично можно учесть стоимость изменения параметра (при проникновении);

β - среднее число деталей или параметров, заменённых при одном проникновении.

Стоимость простоев можно описать соотношением

$$C_{пр} = C_п\, \tau_b\, \theta_0 (1\text{-}e^{-\theta/\theta 0}) / T_0 , \qquad (2.3.9)$$

где $C_п$ – потери за час простоя;

θ_0 - срок окупаемости.

Стоимость гибели имущества ($C_{ги}$) с вероятностью гибели $Р_г$=1-$К_г$

Определяется

$$C_г = C_{ги} (1\text{-}К_г) . \qquad (2.3.10)$$

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

$$C_{ку} = C_{кку} + C_{ркy} + C_{прку} + C_{гку} , \qquad (2.3.11)$$

где $C_{кку} = C_к + C'_{кку}$

$C'_{кку}$ - стоимость ЗМ , которую можно выразить полученным ранее [66] соотношением

$$C'_{кку} = A D^{l} / [(1-B)^{k} К_{г} /К_{гу}) + t \log_{c}[A / (1-B)^{k} К_{г} /К_{гу}] \qquad (2.3.12)$$

Здесь B – критерий объективности контроля;

D – коэффициент, определяемый в зависимости от вида ЗМ, выполняемых им функций (контроль работоспособности, отыскание неисправностей и проникновений, прогнозирование);

l – коэффициент, зависящий от сложности контроля определяющих параметров, от степени автоматизации;

k – коэффициент, зависящий от способа обработки информации с датчиков;

t – коэффициент, зависящий от ЗМ , от вида индикации;

c – определяется ограничениями по стоимости, массе и габаритам, предъявляемыми к РЭС.

Все остальные составляющие соотношения (2.3.11) также изменяются, так как обычно

$$К_{гку} \supseteq К_{г} \; ; \qquad \tau_{вку} < \tau_{в} \; ; \qquad C_{раб\,ЗМ} < C_{раб}.$$

При этом предполагаем, что надёжность ЗМ значительно выше, чем РЭС.

Можно использовать условие целесообразности внедрения ЗМ определённого типа в РЭС в виде [66]

$$К_{гку} > К_{г} \quad при \quad C_{ЗМ} = C \qquad (2.3.13)$$

или

$$К_{гку} = К_{г} \quad при \; C_{ЗМ} < C \; , \qquad (2.3.14)$$

Из таких принципов и необходимо исходить при обосновании целесообразности использования ЗМ и при выборе варианта ЗМ.

С точки зрения экономики наши соотношения могут показаться не строгими, так как в последнем случае (2.3.6) мы рассматриваем не приведённые затраты, а величины, называемые стоимостью. Однако эта

вольность допустима, на наш взгляд, при сравнении аппаратуры примерно одного класса и для количественной оценки в первом приближении.

Достаточную точность позволяет получить соотношение (2.3.5) при определении эффективности. Для оценки значений составляющих это соотношение, при отсутствии необходимых данных, можно использовать приближённые математические модели (2.3.7-10,12) . Кстати, и $С_к$ можно заменить $П_{из}$ и $К_м$. Используя приведённые выше соотношения, связывающие характеристики надёжности РЭС и аппаратуры корпоративных сетей со стоимостью, можно попытаться найти такие характеристики надёжности, с которыми РЭС и аппаратуры корпоративных сетей за определённое время эксплуатации будет иметь наименьшую общую стоимость[26,36,37].

Эти методики внедрены (см. Приложение 5.6.7) разработаны программные продукт и расчёты для основной части электронных сетей Иордании и будет внедрены в корпоративные компьютерные телекоммуникационные сети, одну из них приводим в приложении (2) .

2.4.Минимизация маршрутизаторов при обеспечении информационной защиты для телекоммуникационных государственных сетей Иордании

Рассмотрим алгоритм поиска и построения маршрутизаторов для обеспечения информационной защиты в сетях[41,64,67,99].

Сначала построим матрицу уровней ***L***[41,67]. Уровнями будем называть ***x*** и ***y*** координаты, на которых лежат ядра. 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 (рис 2.4.1).

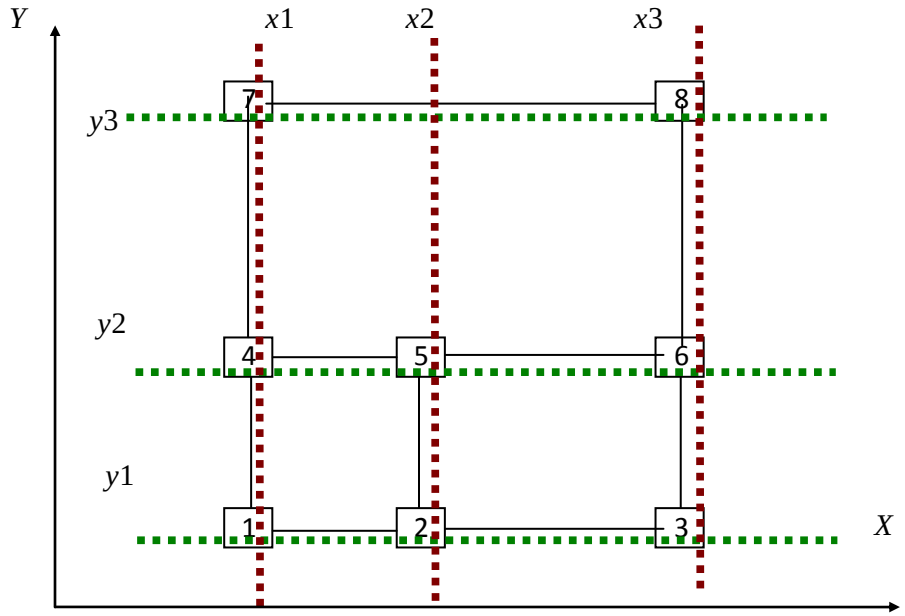


Рис 2.4.1. Уровни ядер в сети.

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 2.4.1).

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

Предложенная нами блок-схема алгоритма показана на рис 2.4.2.

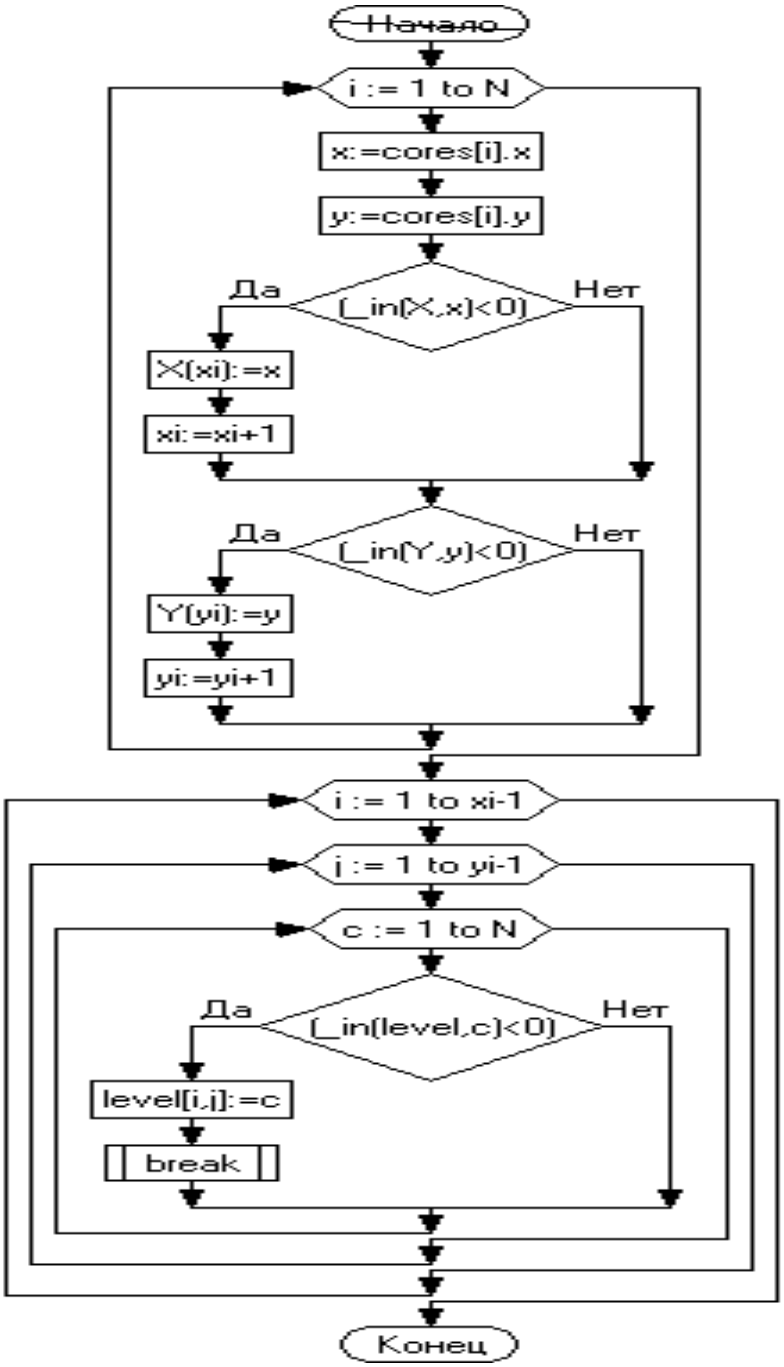


Рис 2.4.2. Блок-схема алгоритма чтобы найти все уровни *x* или *y*.

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”.

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” a, соответственно $L(i + 1, j)$ и $L(i, j + 1)$, c и b (см рис. 2.4.2). Теперь остается найти точку d.

Для этого начиная с $L(i + 1, j)$ двигаемся вниз, до уровня $L(i, j + 1)$ и если находим ядро $L(i + 1, j + k)$ связанное с $L(i, j + 1)$, это и есть искомая точка d. Если на уровне $i + 1$ не нашли точку d , переходим к следующему уровню $i + 2$ и т.д. пока не будет найдена точка или же не закончатся ядра. Индексы i,j пробегают от 1 до $X – 1$ и от 1 до $Y – 1$, соответственно. Так как очевидно, что ядра находящиеся на последних уровнях не могут быть началами маршрутизаторов.

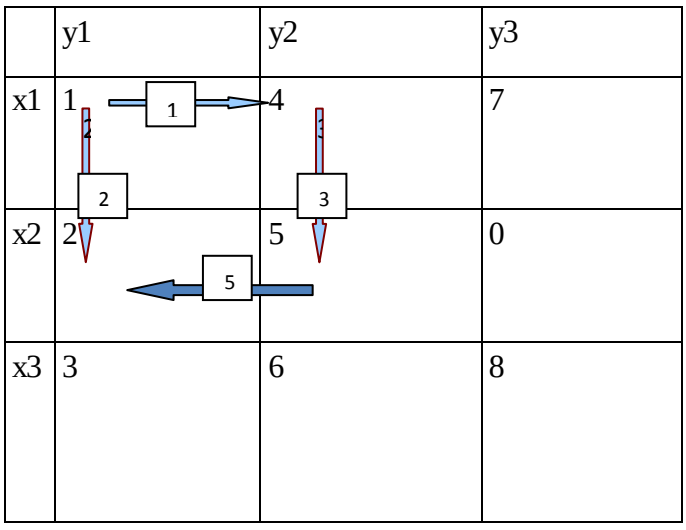


Рис.2.4.3. Номера на стрелках указывают порядок действий.

Возьмем ядро 1. Оно находится на уровне *x*1 и *y*1. Ищем его соседей с слева и сверху. Это ядра 4 и 2 если с ними есть связь, то это возможно маршрутизатор. Далее начинаем двигаться от ядра 4, находящимся на уровне *x*1, *y*2 вниз до уровня на котором находится ядро 2 те *x*2. Там есть ядро 5, которое связано с 2 и 4, следовательно маршрутизатор построен, и он состоит из ядер 1,2,4,5. По аналогии строим маршрутизатор 2,3,5,6 и 4,6,7.8.

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 , что бы не пропадали ядра (см. пример на рис. 2.4.4). И длина пути не оказалась больше максимально разрешенной длины пути *D*.

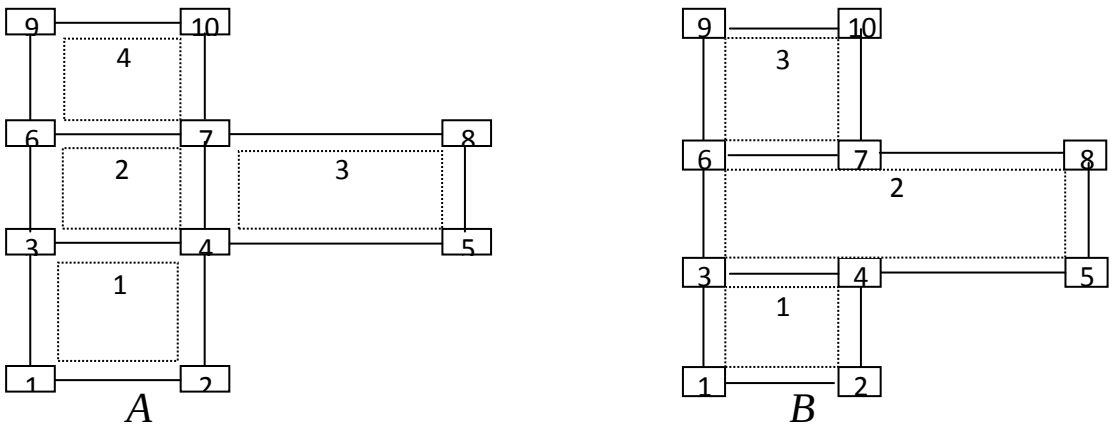


Рис 2.4.4. Объединение маршрутизаторов. *A* - до объединения, *B* - после.

На рис.2.4.4 изображены 10 ядер, связи между ними и 4 маршрутизатора.

Блок-схема алгоритма построения маршрутизаторов и их минимизации.

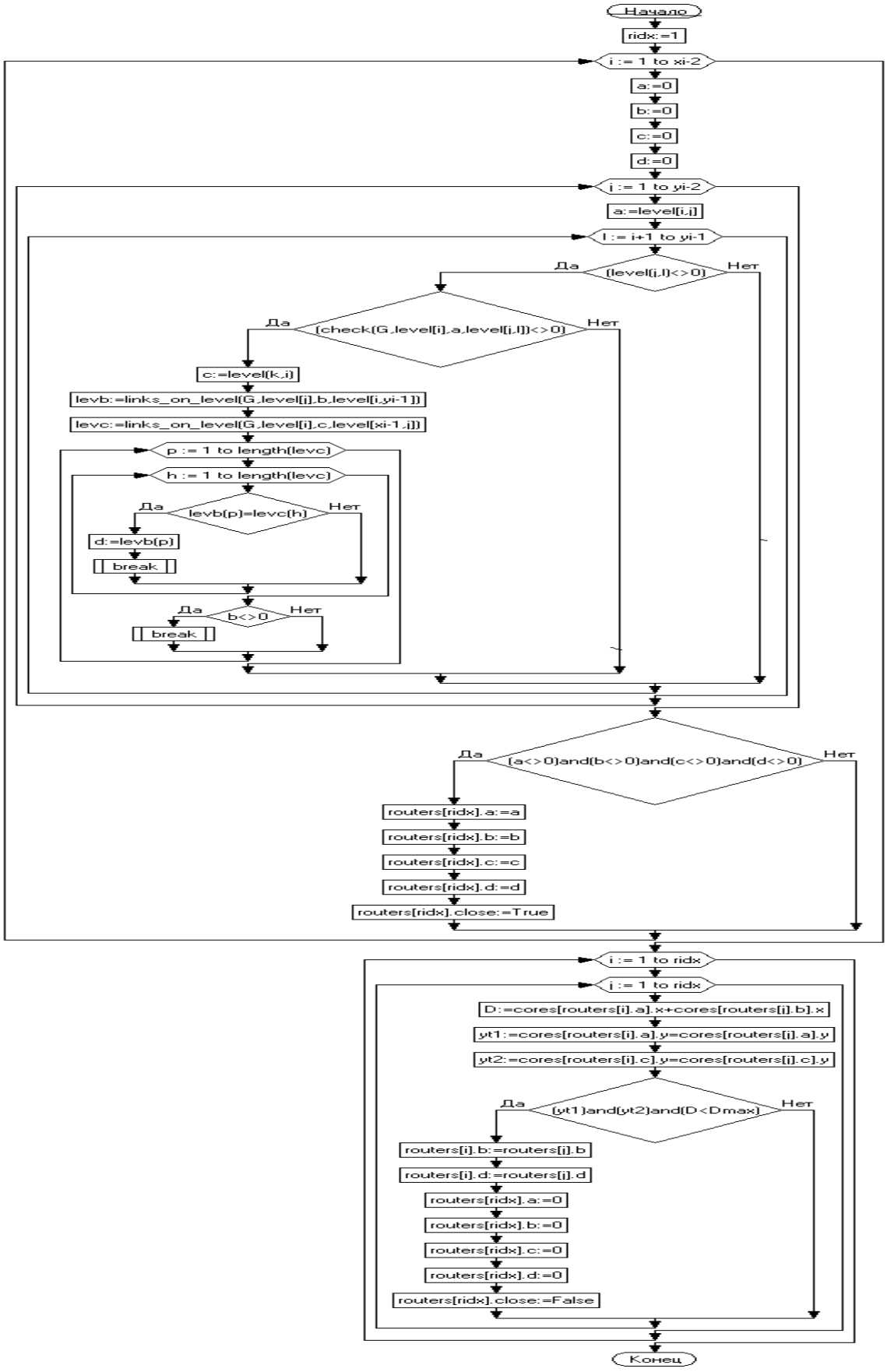


Рис 2.4.5. Алгоритм построения маршрутизаторов и их минимизации.

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.

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, на рис(2.4.5) . 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 было 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. По существу, каждый порт ядра должен быть смоделирован отдельным узлом в потоковом графе, чтобы решить этот вопрос[41,67,99].

2.5. Выводы по главе 2

1. Необходимо оценить и обосновать повышение эффективности мероприятий по защите от несанкционированного доступа для каждого конкретного учреждения и предприятия в зависимости от задач стоящих перед ними в каждом отдельном случае и, в частности, для повышения его конкурентоспособности, поскольку это наиболее точные и достоверные оценки. Наилучшие критерии по точности и достоверности – экономические. Разработанные нами методики обеспечивают решение этих проблем.
2. Для этих случаев важно разработать защищенный информационный канал.
3. Для учреждений и предприятий в конечном итоге важна эффективность сети связи в зависимости от срывов (в том числе и от проникновений в нее). Разработанные нами расчетные методики позволяют решить эту проблему.
4. Приведен один из подходов к математическому анализу эффективности защитных мероприятий, который затем может быть использован при математическом моделировании.
5. Разработаны программные продукты (см. приложения 2), и расчёты для основной части сетей Иордании и корпоративных компьютерных телекоммуникационных сетей с малоразрядными кодами.
6. Разработаны методики и алгоритмы минимизация маршрутизаторов на этапе проектирования что позволяет уменьшить аппаратурные затраты более чем в 2 раза (см. Приложения 5).

ГЛАВА 3. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ПРОНИКНОВЕНИЙ В КАНАЛ КОРПОРАТИВНОЙ СЕТИ ИОРДАНИИ И ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СЕТЯХ С МАЛОРАЗРЯДНЫМИ КОДАМИ

3.1. Пути оптимизации информационной защиты радиосисмем от несанкционированного доступа для государственных сетей Иордании

3.1.1. Выбор контролируемых параметров по максимальным значениям (с учетом защиты канала)

Выбор параметров для контроля по информативным признакам достаточно сложен и требует обширных фактических данных. Для инженерных расчетов приемлемыми являются методы линейного и динамического программирования[66,117].

Рассмотрим применение линейного программирования для определения номенклатуры контролируемых параметров с целью получения максимальной информации о техническом состоянии (защите) канала при заданном коэффициенте готовности и выполнении ряда ограничений (например стоимость контроля, масса, габариты и т.д.).

Решение этой задачи возможно при определенных допущениях. Поставим задачу в терминологии линейного программирования. Найти подмножество контролируемых параметров ω множества Ω, максимизирующее при соблюдении ограничений линейную функцию B или

$$B_{\omega} = \max_{\omega \in \Omega} \{B / g_s \le G_s; s = 1,2\ldots\}, \qquad (3.1.1.1)$$

где gs – достигнутое значение по s-му ограничению; Gs – ограничение на выбор состава контролируемых параметров.

Если рассматривать применение в качестве максимизируемой функции критерия объективности контроля в виде

$$B_\omega = \sum_{i \in \omega} b_i \qquad (3.1.1.2)$$

где,

$$b_i = \frac{I_i}{\sum_{i \in \omega} I_i} \qquad (3.1.1.3)$$

$$I_i = -\frac{\lambda_i}{\Lambda} \log_2 \frac{\Lambda}{\lambda_i} - \left(1 - \frac{\lambda_i}{\Lambda}\right) \log_2 \frac{1}{\left(1 - \frac{\lambda_i}{\Lambda}\right)} \qquad (3.1.1.4)$$

где λi – интенсивность проникновений в i-й параметр;

Λ – интенсивность проникновений в канал – $\Lambda = \sum_{i \in \Omega} \lambda_i$

Не меняя практически сути рассуждений, можно принять $bi = \lambda i / \Lambda$, что значительно упрощает вычисления. Принимаются следующие допущения, пригодные для широкого класса каналов:

- надежность параметров не изменяется при введении КУ;
- параметры взаимонезависимые ;
- для всех параметров выполняется

$\lambda i << \Lambda$; (3.1.1.5)

- в среднем время отыскания неисправного элемента τот i (без КУ) больше, чем время устранения неисправности или проникновения τус i этого элемента;

$$\tau_{от\,i} + \tau_{ус\,i} = \tau_{в\,I}$$

– время восстановления i-го элемента; для всех элементов выполняется условие

$$\tau_{от\ ку\ i} << \tau_{ус\,i} \qquad (3.1.1.6)$$

.

3.1.2. Выбор контролируемых параметров по заданному коэффициенту готовности

В качестве обязательного ограничения можно потребовать получение какой-либо характеристики надежности заданного значения, например, коэффициента готовности, в виде [47, 66]

$$\sum_{i\in\omega} Z_i\gamma_i + \sum_{j\in\omega} Z_i\gamma_i \le \frac{1-K_{гз}}{K_{гз}} \qquad (3.1.2.1)$$

$$\overline{\omega}\cup\omega = \Omega, \quad \overline{\omega}\cap\omega = \varnothing;$$

где $Z_i \neq Z_j$

$$Z_i\,,\, Z_j = \begin{cases} 0, \\ 1; \end{cases} \qquad (3.1.2.2)$$

$$\gamma_i = \lambda_i\,(\tau_{от\ ку\ i} + \tau_{ус\ i});$$

$$\gamma_j = \lambda_j\,(\tau_{от\ j} + \tau_{ус\ j});$$

$$\lambda_j \approx \lambda_i\,;\ \ \tau_{ус\ j} \approx \tau_{ус\ i}\,. \qquad (3.1.2.3)$$

В качестве λi можно использовать вероятность отказа, в предположении qi ≡ λi. Формализуем условие задачи.

Определить набор Z = (z1, z2, …, zn), максимизирующий функцию

$$\sum_{i\in\omega} Z_i b_i + \sum_{j\in\omega} Z_j\, b_j\ ,$$

$$\omega\cap\overline{\omega} = \varnothing, \quad \omega\cup\omega = \overline{\Omega}, \qquad (3.1.2.4)$$

при условиях

$$\sum_{i\in\omega} Z_i\gamma_i + \sum_{j\in\omega} Z_i\gamma_i \le \frac{1-K_{гз}}{K_{гз}};$$

$$\sum_{i\in\omega} Z_i g_{si} + \sum_{j\in\omega} Z_j\, g_{sj} \le G_s\,;$$

$$Z_i\,,\, Z_j = \begin{cases} 0, & Z_i \neq Z_j\ . \\ 1; \end{cases} \qquad (3.1.2.5)$$

Покажем применение расчетных соотношений на примере Иордании.

Пример. В коммуникациях компьютерной сети имеется 10 определяющих параметров. Необходимый Кгз = 0,978, максимальная стоимость КУ G1 = 150 условным единицам, максимальная масса КУ G2 = 80 условным единицам. Данные о параметрах сведены в табл. 3.1.2.1.

Все параметры канала контролировать нельзя, так как нарушаются граничные условия . Определяются величины I_i и $\sum_{i\in\omega} I_i$

$$\sum_{i=1,}^{10} I_i = 0,45+0,23+0,71+0,4+0,6+0,4\,5+0,23+0,23+0,05+0,71=4,06,$$

После чего находятся коэффициенты bi и γi, γj. Все показатели сводятся в таблице. 3.1.2.2.

Таблица 3.1.2.1.Параметры нашего примера

Параметр	Значение и номер параметра										Мно-жи-тель
	1	2	3	4	5	6	7	8	9	10	
λ_i , 1/ч	1	0,5	2	0,8	1,5	1	0,5	0,5	0,2	2	10^{-2}
τ_{bi}, ч	2	4	6	2	1	0,2	4	2	2	2	10^{-1}
τ_{yci}, ч	1,6	1	4,8	1,4	0,8	0,16	1	0,5	0,6	1,6	10^{-1}
g_{1i}, усл.ед.	10	20	10	30	20	10	10	10	20	40	–
g_{2i}, усл.ед.	5	10	20	20	20	10	5	10	5	5	–

Таблица 3.1.2.2.Расчетные значения нашего примера.

Параметр	Значение и номер параметра										Множитель
	1	2	3	4	5	6	7	8	9	10	
b_i	0,11	0,06	0,17	0,1	0,15	0,11	0,06	0,06	0,01	0,17	–
γ_i	1,6	0,5	9,6	1,12	1,2	0,16	0,5	0,25	0,12	3,2	10^{-3}
γ_j	2	2	12	1,6	1,5	0,2	2	1	0,4	4	10^{-3}

Требуется найти набор

$Z = \{ z_1, z_2, \ldots, z_{10}\}$

$\omega \in \Omega$,

максимизирующий линейную функцию

$$0{,}11\, z_1 + 0{,}06\, z_2 + 0{,}17\, z_3 + 0{,}1\, z_4 + 0{,}15\, z_5 + 0{,}11\, z_6 + \\ + 0{,}06\, z_7 + 0{,}06\, z_8 + 0{,}01\, z_9 + 0{,}17\, z_{10}\,, \qquad (3.1.2.6)$$

при условиях

$$(1{,}6\, z_1 + 0{,}5\, z_2 + 9{,}6\, z_3 + 1{,}12\, z_4 + 1{,}2\, z_5 + 0{,}16\, z_6 + 0{,}5\, z_7 + 0{,}25\, z_8 + 0{,}12\, z_9 + \\ + 3{,}2\, z_{10})_{i\in\omega} + (2\, z_1 + 2\, z_2 + 12\, z_3 + 1{,}6\, z_4 + 1{,}5\, z_5 + 0{,}2\, z_6 + 2\, z_7 + 1\, z_8 + 0{,}4\, z_9 + \\ + 4\, z_{10})_{j\in\omega} \le 22{,}5;$$

$$10\, z_1 + 20\, z_2 + 10\, z_3 + 30\, z_4 + 20\, z_5 + 10\, z_6 + 10\, z_7 + 10\, z_8 + 20\, z_9 + 40\, z_{10} \le 150;$$

$$5\, z_1 + 10\, z_2 + 20\, z_3 + 20\, z_4 + 20\, z_5 + 10\, z_6 + 10\, z_7 + 10\, z_8 + 5\, z_9 + 5\, z_{10} \le 80.$$

$$Z_i\,,\ Z_j = \begin{cases} 0, & Z_i \neq Z_j \\ 1; \end{cases} \qquad (3.1.2.7)$$

Решая задачу методом направленного полного перебора, получаем оптимальный набор контролируемых параметров при выполнении граничных условий и максимальном Bω= 0,81.

Предложенная методика при ее наглядности и универсальности обладает следующими недостатками: большой объем вычислений при увеличении числа параметров (более 10), особенно при близости их характеристик; сложность приведения к задаче линейного программирования из-за зависимости значения величины γ от выбора Z; трудности разработки вычислительного алгоритма для ПК. В связи с этими недостатками приведенные соотношения целесообразно применять

только для каналов с малым числом параметров (единицы). Однако, преобразуя к виду

$$\sum_{i\varepsilon\Omega} Z_i\gamma_{cti} \geq \frac{К_{гз} - К_г}{К_г\ К_{гз}}, \qquad (3.1.2.8)$$

или

$$\sum_{i\varepsilon\Omega} Z_i\gamma_{ст\,I} \geq \Lambda(\tau_в - \tau_{вз}), \qquad (3.1.2.9)$$

или

$$\sum_{i\varepsilon\Omega} Z_i\gamma_{ст\,I} \geq \Lambda\tau_в - \left(\frac{1 - К_{гз}}{К_{гз}}\right), \qquad (3.1.2.10)$$

где Λ – интенсивность отказов канала;

$\tau_в$ – среднее время устранения одной неисправности или проникновения;

$\tau_{вз}$ – заданное время восстановления;

$$\gamma_{ст\,i} = \lambda_i\tau_{ст\,i} \approx q_i\ \tau_{ст\,i}, \qquad (3.1.2.11)$$

Добиваемся отсутствия зависимости γ от выбора Z. Поэтому сравнительно просто можно придти к задаче линейного программирования с булевыми переменными в следующей математической постановке.

Определить набор $Z = (Z_1, Z_2, \ldots, Z_n)$, максимизирующий функцию

$$\sum_{i\varepsilon\Omega} Z_i\,В_i$$

при условиях

$$\begin{cases} \sum_{i\varepsilon\Omega} Z_i\gamma_{ст\,i} \geq \left(\frac{1 - К_{гз}}{К_{гз}}\right), \\ \sum_{i\varepsilon\Omega} Z_i g_{si} \leq G_s; \\ Z_i = \begin{cases} 0, \\ 1, \end{cases} \\ В_i > 0;\ \gamma_{ст\,i} > 0;\ g_{s\,i} > 0; \end{cases}$$

При такой постановке задача может быть решена методами линейного программирования с булевыми переменными, в том числе и на ПК.

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

Рассмотрим задачу выбора для случая, когда параметры взаимозависимы. Причем оптимальным считается такой набор, при контроле которого достигается максимальная апостериорная вероятность безотказной работы и соблюдается условие ограничения (стоимость контроля, время и т.д.).

Задачу выбора оптимального набора контролируемых параметров при ограничении можно решить методами сокращенного перебора. Сокращение перебора достигается использованием специальных правил, позволяющих исключать заведомо неоптимальные наборы. Такие алгоритмы широко приведены в литературе, но они, на наш взгляд, слишком сложны для применения в инженерной практике.

Приведем [66, 91, 94] наш более простой алгоритм, пригодный для определения набора контролируемых параметров каналы сетей Иордании.

Постановка задачи

Система состоит из N элементов. В каждый момент времени возможен отказ лишь одного элемента (одно проникновение). Работоспособность каждого элемента не зависит от состояния других. Отказ любого элемента вызывает выход из зоны допуска значения, по крайней мере, одного из M параметров.

Известные априорные вероятности q_i отказе i-го элемента и для каждого к-го параметра $\pi_к$ определено подмножество $S_к$ элементов, охваченных контролем этого параметра. Другими словами, величиной $S_к$ можно характеризовать ненадежность к-го параметра.

Известны затраты $g_к$ на контроль каждого параметра. При этом предполагается, что затраты g(w) на контроль любой совокупности w параметров слагаются из суммы затрат на контроль каждого параметра из этой совокупности.

Требуется из всех совокупностей (наборов) w , у которых $g(w) \le G_s$ - допустимых планов, (где G_s – s-ое ограничение на проведение контроля) выбрать ту совокупность, при которой вероятность безотказной работы устройства после проведения контроля (диагностики) была бы наибольшей.

Решение

Обозначим: $p_к$ – вероятность безотказной работы тех элементов, у которых контролируется к-й параметр ($q_к=1-p_к$). Вероятность безотказной работы устройства перед контролем

$$P^{(0)} = \prod_{i=1}^{N} P_i = \prod_{i=1}^{N} (1-q_i) \approx 1 - \sum_{i=1}^{N} q_i \qquad (3.1.3.1)$$

При

$$\sum_{i=1}^{N} q_i < 1. \qquad (3.1.3.2)$$

Взаимосвязь параметров и элементов задается матрицей вида

$$\begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1K} & \dots & a_{1M} \\ a_{21} & a_{22} & \dots & a_{2K} & \dots & a_{2M} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{iK} & \dots & a_{iM} \\ \vdots & \vdots & & \vdots & & \vdots \\ \cdot & \cdot & & \cdot & & \cdot \\ a_{N1} & a_{N2} & \dots & a_{NK} & \dots & a_{NM} \end{Vmatrix} \qquad (3.1.3.3)$$

элементы которой определяются из условия

$$a_{iк} \begin{cases} 0, \text{ если } i \notin \pi_к; \\ \\ 1, \text{ если } i \in \pi_к,, \end{cases} = \quad (3.1.3.4)$$

где i – номер элемента;

к – номер параметра.

При этом параметры нумеруются так, чтобы соответствующие им затраты составляли неубывающий ряд

$g_1 \le g_2 \le \ldots \le g_м$.

(Впоследствии предпочтительно начинать выбор параметров слева).

При продолжительном результате контроля к-го параметра, вероятность безотказной работы всех элементов, от которых зависит к-й параметр, принимается равной единице. В этом случае вероятность безотказной работы всей системы определится выражением

$$P^{(к)} = \frac{P^{(10)}}{P_к},$$

где

$$P_к = \prod_{i \in \pi_к} P_i \approx 1 - \sum_{i \in \pi_к} q_i = 1 - S_к. \quad (3.1.3.5)$$

При этом вероятность безотказной работы системы возрастет на величину

$$\Delta P^{(к)} = P^{(к)} - P^{(0)} = \frac{P^{(0)} S_к}{1 - S_к}.$$

Предполагается, что затраты $q_к$ и ограничение G_s таковы, что сумма любых двух значений затрат больше G_s. Тогда для контроля, очевидно, надлежит выбирать лишь один параметр. Этим параметром будет тот, у которого сумма $S_к$ будет наибольшей, а следовательно и приращение $\Delta P^{(к)}$ также наибольшее. Если таких параметров несколько, то из них надо выбрать тот, у которого произведение $(1-S_к)q_к$ – наименьшее и, следовательно, приращение вероятности, приходящееся на единицу затрат – наибольшее

$$V^{(к)} = \frac{\Delta P^{(к)}}{g_к} = \frac{P^{(0)}S_к}{g_к(1-S_к)} .$$

Если систему проконтролировать некоторой совокупностью w приборов (π_w) и затраты при этом $g(w) < G_s$, то вероятность безотказной работы системы примет значение

$$P^{(w)} = \frac{P^{(0)}}{P_w} ,$$

где $$P_w = \prod_{i \in uк \in w} P_i \approx 1 - \sum_{i \in uк \in w} q_i = 1 - S_w. \qquad (3.1.3.6)$$

При этом общий множитель p_i (или общее слагаемое q_i) берется лишь один раз. Вероятность безотказной работы системы увеличится при этом на величину

$$\Delta P^{(w)} = P^{(0)} - P^{(w)} = \frac{P^{(0)}S_w}{1 - S_w} .$$

Если при фиксированном числе параметров все наборы w таковы, что $g(w) + g_l > G_s$ и $l \notin w$, то из всех наборов оптимальным будет тот, у которого сумма S_w – наибольшая, а, следовательно, и приращение вероятности будет наибольшим. Если окажется несколько наборов с

одинаковой наибольшей суммой S_w , то оптимальным из них будет тот, у которого величина

$$V^{(w)} = \frac{\Delta P^{(w)}}{g(w)} = \frac{P^{(0)} S_w}{g(w)(1-S_w)}$$

наибольшая. Таковым будет набор, у которого произведение $g(w)(-S_w)$ – наименьшее.

Алгоритм

Рациональный набор контролируемых параметров определяется в следующей последовательности:

1-й ш а г. Параметры, у которых $g_к > G_s$ не рассматриваются. Для оставшихся параметров вычисляются $S_к$ и находится наибольшая из них $S_к^{(0)}$. Если таких параметров несколько, то из них выбирается тот, у которого $R_к = g_к(-S_к)$ – наименьшее. Обозначим этот параметр π_1^0.

2-й ш а г. Исключаются из дальнейшего рассмотрения все параметры, у которых $g_к = G_s$ (кроме π_1^0, если $g_1^0 = G_s$). Из оставшихся параметров формируются наборы по два параметра: $(\pi_1,\pi_2)(\pi_1,\pi_3) \ldots (\pi_{м-1},\pi_м)$. Все пары $(\pi_к,\pi_l)$, у которых $g_2 = g_к + g_l > G_s$ не рассматриваются. Вычисляются

$$S_{кl} = \sum_{i \in \pi_к \cup \pi_l} q_i \quad [(l, к) = 1, 2, \ldots, M, l \neq к]$$

и находится наибольшая из них $S_{кl}^{(0)}$. Если таких пар несколько, то из них выбирается та, у которой $R_{кl} = (g_к + g_l)(1 - S_{кl})$ – наименьшее. Обозначим эту пару π_2^0.

m-й ш а г. Процесс продолжается до сочетаний по $m \leq M$ параметров, если еще $g_{w \to M} \leq G_s$. Из полученных наивыгоднейших наборов π_1^0, π_2^0, …, π_m^0 выбирается тот, у которого наименьшее

$$R_w = \sum_{к \in w} q_к \ (1 - S_w) .$$

Соответствующий набор параметров есть решение поставленной задачи. При этом вероятность безотказной работы системы после проведения диагностики достигает наибольшего значения

$$P_{max} = \frac{P^{(0)}}{1 - \max S_w}.$$

Точное решение задачи по предлагаемому алгоритму при больших M и N (несколько десятков) становится весьма громоздким. Можно указать приближенные методы, которые позволяют получить вполне приемлемую для инженерной практики точность.

Приближенный комбинированный метод, в котором применены предыдущие методы и основные идеи метода ветвей и границ.

Определяется базовый набор $w_Б^0$, состоящий их n параметров при $g(w_Б^0) \le G_s$. В наборах $w_Б^0$ и $\overline{w_Б^0}$ ($w_Б^0 \cap w_Б^0 = \varnothing$ и $\overline{w_Б^0} \cup w_Б^0 \subseteq M$) отыскиваются такие параметры, чтобы

$$V^{(к \in wБ^0)} > V^{(l \in wБ^0)} \qquad (3.1.3.7)$$

Комбинированный метод, очевидно, самый эффективный из рассмотренных и позволяет наиболее быстро подойти к решении задачи.

При

$$g(w_Б^1) \le G_s;$$

$$к \in w_Б^1; \qquad (3.1.3.8)$$

.

$$Г \in w_Б^1.$$

Такие операции проводятся до тех пор пока находятся параметры, удовлетворяющие условиям (3.1.3.7 и 3.1.3.8). При этом оптимальным наборов w_0 из $\{w_Б^0, w_Б^1, w_Б^2, \ldots, w_Б^m\}$ считается тот, у которого

$$P(w_0) = \max \{P(w_Б^0), P(w_Б^1), P(w_Б^2), \ldots, P(w_Б^m)\}.$$

Приведем характеристики числа переборов вариантов без учета допустимости и перспективности планов (табл.3.1.3.1).

Следует отметить, что с ростом M и n различие в числе переборов для этих методов быстро возрастает.

Таблица 3.1.3.1 для случая структуры нашего примера изображенной на рис(1.6.1).

Метод (алгоритм)	Максимальное число переборов	n=5 **M=7**
Полный перебор	$\leq \sum_{i=1}^{M} C_м^i$	127
А	$\leq C_м^n$	21
Б	$\leq (nM - \sum_{i=0}^{n-1} i)$	25
Алгоритм Р.Р.Убара	$<(C_м^{]M/2[} + C_м^{]M/2[+1})$	70
В	$\leq \begin{cases} n \ / \ n \leq м - n \\ (M-n) \ / \ n \geq M - n \end{cases}$	2

По простоте алгоритма и по элементарности вычислений, а также по быстроте решения наиболее предпочтительным, на наш взгляд, является метод В. Используя понятие веса (важности) параметра можно заменить в матрице (3.1.3.3) величину $a_{iк}$ на $h_{iк}$.

При этом $\sum_{i=1}^{M} h_{ik} = 1,$

а h_{ik} показывает (относительно) как сильно влияет i-ый элемент (точнее параметры элемента) на к-ый параметр.

Такая замена особенно эффективна при преобладающем количестве параметрических отказов.

Заметим, что не меняя сущности метода, можно заменить величину q_i на $\lambda_i \tau_{bi}$ или на τ_{bi}/τ_{cpi} (где λ_i – интенсивность отказов i-го элемента; τ_{cpi} – среднее время восстановления i-го элемента). При этом в выражении (3.1.3.1) $P^{(0)}$ будет иметь смысл коэффициента готовности.

Проиллюстрируем изложенные методы решения задачи на простых примерах.

Исходные данные приведены в табл.3.1.3.2. ограничение G_y=7.

Таблица 3.1.3.2 для случая структуры изображенной на рис(1.6.1).

№	q_i x 10^3	π_1	π_2	π_3	π_4	π_5
		затраты на контроль				
		2	2	2	3	3
1	3		3			
2	5			5	5	5
3	4	4				4
4	4			5		
5	4				4	
$S_к$ x 10^3	20	4	3	9	9	9
1 - $S_к$	0,980	0,996	0,997	0,991	0,991	0,991
$R_к = g_к (1 – S_к)$		-	-	1,882	-	-

Пример 1. Из табл.3.1.3.2 видно, что предпочтительным для контроля является параметр π_3, то есть

$$\pi_{1^\circ} = \pi_3; \quad P^{(3)} = \frac{0,980}{0,991} = 0,988.$$

Сочетания по два параметра для определения π_{2° представлены в табл.3.1.3.3.

Из нее следует, что предпочтительным для контроля является сочетание параметров $\pi_3\pi_4 = \pi_{2^\circ}$;

$$P^{(34)} = \frac{0,980}{1 - 0,013} = 0,993$$

Таблица 3.1.3.3 для случая структуры нашего примера и рис(1.1.1).

№	$q_i \times 10^3$	12	13	14	15	23	24	25	34	35	45
		затраты на контроль $g_{(2)}$									
		4	4	5	5	4	5	5	5	5	6
1	3					3	3	3			
2	5		5	5	5	5	5	5	5	5	5
3	4	4	4	4	4			4		4	4
4	4					4			4		
5	4								4		4
$S_{кl} \times 10^3$		7	9	9	9	12	8	12	13	9	13
$(1 - S_{кl}) \times 10^3$		993	991	991	991	988	992	988	987	991	987
$(1 - S_{кl}) \times g(2)$		3,952									

Сочетания по три параметра для определения π_{3° представлены в табл.3.1.3.4.

Таблица 3.1.3.4 для случая структуры нашего примера.

№	$q_i \times 10^3$	123	124	125	134	135	145	234	235	245	345
		затраты на контроль $g_{(3)}$									
		6	7	7	7	7	8	7	7	8	8
1	3	3	3	3		5		3	3		
2	5	5	5	5	5	4		5	5		
3	4	4	4	4	4				4		
4	4	4			4			4	4		
5	4		4		4			4			
$S_3 \times 10^3$		16	16	12	17	9	-	16	16	-	-
$(1 - S_3) \times 10^3$		984	984	988	983	991		984	984		

Примечание: наборы 145, 245 и 345 не рассматриваются, так как для них g(3) = 8>7.

Из табл.3.1.3.4 получаем рациональный набор $\pi_{3\circ}=\pi_1\pi_3\pi_4$.

При этом

$$P^{(134)} = \frac{0{,}980}{1 - 0{,}017} = 0{,}997.$$

Любое сочетание по 4 прибора дает g(w)>7.

Сравнивая $P^{(3)}$, $P^{(34)}$ и $P^{(134)}$, получаем оптимальный набор ($\pi_1\pi_3\pi_4$).

Пример 2. Для тех же числовых данных решим задачу I-ым приближенным методом. В нашем случае

$$M=5;\ g_c = \frac{12}{5} = 2{,}4;$$

$$n = \left[\frac{7}{2{,}4}\right] + 1 = 3$$

Составляется табл.3.1.3.4 и из нее находится $\pi_{3^\circ}=\pi_1\pi_3\pi_4$.

Пример 3. Решаем 2-м приближенным методом. Из табл.3.1.3.2 имеем $\pi к_{1^\circ}=\pi_3$. После этого объем табл.3.1.3.3 сократится, то есть в ней рассматриваются лишь сочетания с параметром π_3 [(31), (32), (34) и (35)].

Минимум произведения $(1\text{-}S_{кl})g(2)$ дает максимум $V^{(кl)}$. Таким образом, как это следует из табл.3.1.3.3, сочетание $\pi к_{1^\circ}\pi к_{2^\circ}=\pi_3\pi_2$.

По этим же причинам сокращается и объем табл.3.1.3.4, так как в ней рассматриваются лишь сочетания с параметрами π_3 и π_2 [(231) , (234) и (235)].

Наименьшее произведение $(1 - S_3)\ g(3)$ соответствует сочетанию $\pi_2\pi_3\pi_1$. Для этого сочетания величина $V^{(к1\,0\quad к2\,0\quad 3\,0)}$ - наибольшая.

Приближенно определенный набор незначительно отличается от ранее найденного и при затратах $g_1 + g_2 + g_3 = 6 < 7$, вероятность безотказной работы $P^{(123)} = 0{,}996$. Такую стратегию мы используем при составлении алгоритма и программы (см. 3.3.1 и Приложение 3,4).

3.1.4. Оценка оптимального времени между проведением функциональных проверок информационного канала

Если вероятность выявления отказов канала или проникновений в него задается с помощью непрерывного контроля Рнк или с помощью контроля Рфк = 1 – Рнк , то значение стационарного коэффициента готовности можно выразить соотношением

$$K_г = \frac{T_о}{T_о + \tau_в + P_{фк}\ T_{фк}/2} \quad \frac{T_{фк}}{T_{фк} + \tau_{фк}}, \qquad (3.1.4.1)$$

где То – среднее время работы канала между отказами;

τв – среднее время существования отказа (τв= τот + τус);

Тфк – среднее время между проведением функционального контроля;

τфк – среднее время проведения функционального контроля.

Функциональный контроль связан с прекращением выполнения аппаратурой поставленной задачи.

Оптимальное значение времени между проведением функционального контроля, при котором обеспечивается максимальный коэффициент готовности, определяется формулой

$$T_{фк} = \sqrt{\frac{2\tau_{фк}(\tau_о + \tau_в)}{P_{фк}}} \qquad (3.1.4.2)$$

Оптимизация блоков контролируемой аппаратуры. Очевидно, что чем на большее число блоков разделен канал, тем лучше ремонтопригодность аппаратуры и, следовательно, коэффициент готовности. В то же время возрастает сложность аппаратуры контроля и больше влияют ее погрешности (и проникновения в канал).

Отсюда вытекает требование целесообразного разбиения канала на блоки с контролируемыми параметрами.

В работе получена формула для определения оптимального количества блоков с контролируемой работоспособностью при условии

$$\tau << t << T_о << T_{кi}, \qquad (3.1.4.3)$$

где τ – средняя длительность нерабочих периодов;

t – рассматриваемый текущий момент времени работы РЭА;

Ткi – среднее время безотказной работы аппаратуры диагностики, относящейся к одному блоку.

Легко видеть, что условие выполняется для широкого класса РЭА и аппаратуры контроля. Оптимальное количество блоков для достижения максимального коэффициента готовности находится по формуле

$$M = \frac{-B + \sqrt{B^2 - 4AC}}{2A}, \qquad (3.1.4.4)$$

где

$$A = (\tau_{ус} + P_и\tau)(\tau + \tau_{ус});$$
$$B = 2\tau_{от}(P_и\tau + \tau_{ус});$$

$$C = \tau_{от}\left[\tau_{от} - \frac{\tau T_{ки}(1-P_и)}{P_{ло}T_о}\right]. \qquad (3.1.4.5)$$

Здесь Ри – вероятность того, что канал используется в любой произвольный момент времени t (не зависит от t);

τот – среднее время отыскания неисправности или проникновения в аппаратуре, не разделенной на блоки;

Рло – вероятность того, что отказ блочного узла аппаратуры диагностики выражается в выдаче неправильной информации об исправном блоке (Рло=1-Рправ, где Рправ – вероятность того, что блочный узел выдает правильную информацию о неисправном блоке при условии, что отказ или проникновение произошли).

3.2. Выигрыш во времени использования канала корпоративной сети за счет уменьшения числа ошибок при отыскании проникновений и защите канала

При диагностике канала выигрыш во времени использования получается не только за счет уменьшения среднего времени на отыскание проникновений и расстроенных параметров, но и за счет уменьшения

повторных информационных потоков (ПИП)[66,117], которые нужны для повышения достоверности корпоративных сетей Иордании.

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 определяется соотношением

$$\tau = \tau_b' + \tau_{пн}, \qquad (3.2.1)$$

где τ_b' - среднее время использования, определенное без учета ПИП;

$\tau_{пн}$ – среднее время использования за счет появления ПИП.

Однако, как правило, собираемые и имеющиеся статистические данные по времени использования канала определяют его как

$$\tau = \tau_b'' + \tau_{пн}, \qquad (3.2.2)$$

Где τ_b - среднее время использования, определяемое из статистических данных;

τ_b'' – среднее время восстановления без учета ПИП, в отличие от τ_b' - неизвестное.

Соотношение (3.2.2) описывает модель использования канала с учетом ПИП в более общей форме, чем (3.2.1). Поэтому все дальнейшие выкладки проводятся в предположении того, что $\tau_{пн}$ определяется из соотношения (3.2.2).

Значение среднего времени использования за счет ПИП можно определить выражением

$$\tau_{пн} = \sum_{i \in \Omega} P_i P_{пн\,i}\, \tau_{пн\,i}, \qquad (3.2.3)$$

где P_i – вероятность отказа i-го элемента;

$P_{пн\ i}$ – вероятность возникновения ПИП, при защите, связанной с проникновением в зоне i-го элемента;

$$P_{пн\,i} = P_{поi} + P_{пуi}; \qquad (3.2.4)$$

где $P_{поi}$ - вероятность ПИП при отыскании проникновения в зоне i-го элемента;

$P_{пуi}$ - вероятность ПИП при устранении проникновения в зону i-го элемента;

$\tau_{пнi}$ - время, потребное на отыскание и устранение ПИП, связанной с отказом i-го элемента;

Ω - множество элементов (параметров) канала.

Для элементов (параметров), диагностика которых проводится автоматически, величина $P_{поi}$ становится равной нулю, так как в этих случаях непосредственно без проверок («ручных»), отказавший элемент заменяется (расстроенный параметр – настраивается).

Поэтому при автоматических мероприятиях по защите канала (АМЗК) время использования за счет ПИП находится из соотношения

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

$$w \cup \overline{w} = \Omega; \quad w \cap \overline{w} = \varnothing \qquad (3.2.5)$$

Здесь w – подмножество диагностируемых элементов.

Выигрыш во времени использования при этом равен

$$\Delta\,\tau_{пн\ АМЗК} = \tau_{пн} - \tau_{пнАМЗК} \qquad (3.2.6)$$

Следовательно, среднее время использования канала при АМЗК определяется как

$$\tau_{в\ АМЗК} = \tau_{в} - \Delta\tau_{пн\ АМЗК}, \qquad (3.2.7)$$

где $\tau_в$ – из выражения (3.1.2) и рассчитывается по статистическим данным по эксплуатации канала.

Ввиду трудности получения оценки величин $P_{пн\,i}$ и $\tau_{пнi}$, пользоваться приведенными соотношениями практически невозможно. Поэтому произведем оценку выигрыша приближенным способом. Вводится величина $P_п$ – вероятность ПИП при защите из-за ошибок обслуживающего персонала, равная

$$P_п = P_{по} + P_{пу}, \qquad (3.2.8)$$

где $P_{по}$ и $P_{пу}$ – вероятности повреждения канала при отыскания и устранении проникновений.

Находится коэффициент повторных неисправностей по формуле

$$K_{пн} = 1 + \frac{P_п}{1 - P_п}. \qquad (3.2.9)$$

В предположении того, что при отказах элементов любых типов величина $P_п$ = const, при АМЗК

$$K_{пнАМЗК} = 1 + \frac{P_{АМЗК}P_{пу} + (1-P_{АМЗК})P_п}{1 - P_{АМЗК}P_{пу} - (1 - P_{АМЗК})P_п} \qquad (3.2.10)$$

–

где $P_{АМЗК}$ - вероятность того, что отказ вызван элементом, контролируемым АМЗК;

$$P_{АМЗК} = \frac{\sum_{i \in w} \lambda_i}{\Lambda}. \qquad (3.2.11)$$

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

$$\Delta \tau_{\text{пн АМЗК}} = \tau_{\text{в}}(K_{\text{пн}} - K_{\text{пн АМЗК}}) . \qquad (3.2.12)$$

При проведение исследований получили результаты 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%), для государственных сетей Иордании.

3.3. Защита от угроз информационной безопасности в телекоммуникационных государственных сетях Иордании

Для разработки и внедрения системы защиты информационной системы (ИС) нужно [6,66,92,93,117]:

1.Оценить, что является угрозами для данной системы, а что – нет.

2.Оценить экономическую эффективность защиты от определенных угроз.

3.Чтобы средства безопасности были максимально эффективными, механизмы защиты должны быть заложены на этапе проектирования ИС и аппаратных средств, а не после внедрения. Внутреннюю защиту обойти сложнее, чем внешнюю.

4.В ходе планирования и реализации мер по защите информации необходимо опираться на Российские и международные стандарты.

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

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

Формализуем данную задачу.

Исходные данные

Обозначим: УГ = *{*$УГ_1$, $УГ_2$, ...,$УГ_M$*}* – множество всех возможных угроз информации в корпоративной информационной телекоммуникационной сети (КИТС);

Ц = *{*$Ц_1$, $Ц_2$, ... , $Ц_N$*}* – множество целей злоумышленника.

Каждая цель представляет собой совокупность угроз, например $Ц_2$ = *{*$УГ_1$, $УГ_3$,... $УГ_{10}$, $УГ_{11}$, $УГ_{12}$, $УГ_{13}$, $УГ_{14}$, $УГ_{16}$, $УГ_{17}$*};*

А=*{*$А_1$, $А_2$, .., $А_P$*}* – множество атак. Для достижения одной и той же цели злоумышленника могут быть предприняты разные атаки, состоящие из одинаковых угроз.

Подчеркнем тот факт, что за время атаки может быть инициировано несколько однотипных угроз;

СЗ = *{*$СЗ_1$, $СЗ_2$, ..., $СЗ_R$*}* – множество средств защиты, которые способны (в различных подмножествах) обнаружить и нейтрализовать соответствующие угрозы с вероятностью P_{ij} (*i* – номер СЗ, *j*- номер угрозы).

Требуется: найти такое подмножество СЗ*ЄСЗ, чтобы атака $А_P$ была нейтрализована.

В качестве *критерия* оптимального множества СЗ* можно взять:

1) минимум вероятности достижения нарушителем какой-либо или всех целей;

2) минимум среднего уровня потерь системы от реализации нарушителем всех целей;

3) максимум вероятности успешного противодействия системой с множеством СЗ* реализации всех целей нарушителем.

По первому и второму критерию задачу целесообразно решать в случае, когда основной целью системы зашиты - максимальное снижение уровня несанкционированного доступа к информации (преобладание программных и аппаратных средств защиты). По третьему критерию –

когда основная задача защиты состоит в максимальном возможном уровне успешного распознавания факта проникновения или действий злоумышленника в информационной телекоммуникационной сети (ИТС) с целью принятия дальнейших мер по противодействия ему (целесообразность использования данного критерия рекомендуется при преобладании средств физической защиты).

Кроме того, данная задача в ряде случаев может решаться по критерию минимума интегрального показателя “стоимость - риск”, выражающего совокупные затраты на организацию защиты информации и соответствующие им потери от действий злоумышленника.

По этим критериям оптимизации защиты информации в корпоративной сети задачи нахождения оптимального состава комплекса средств защиты (нахождения оптимального $СЗ*$) могут быть сформулированы следующим образом [66,91-93].

Задача 1. Критерий минимум вероятности достижения злоумышленником своих целей.

Определить такие значения $x_i (i = \overline{1,R},$ x_i - номер СЗ), что

$$P(*) = \min_x \prod_{i=1}^{N} P_i^{зл} \ ,$$

при ограничениях:

$$C(СЗ*) \le C_{доп};$$

$$P_i^{зл} \le P_i \, доп$$

Где $P_i^{зл}$ - вероятность достижения злоумышленником i-й цели;

$C(СЗ*)$ - суммарная стоимость выбранных СЗ;

$C_{доп}$ – максимально допустимое значение стоимости систем защиты;

$P_i \, доп$ - допустимое значение вероятности реализации злоумышленником i-ой цели;N – количество целей злоумышленника.

Задача 2. Критерий - максимум вероятности успешного противодействия системы защиты (отобранных в комплекс средств защиты) целям злоумышленника. Определить такие значения

$$P(СЗ^*) = \max_x \prod_{i=1}^{N} (1 - P_i^{зл})\ x_i (i = \overline{1,R},\quad x_i \text{ - номер СЗ}),$$

что при ограничениях:

$$C(СЗ^*) \le C_{доп};$$

$$P_i^{зл} \le P_i\ доп$$

Задача 3. Критерий – минимум среднего уровня потерь от реализации целей нарушителя.

Определить такие значения x_i , что

$$P(СЗ^*) = \min_x \sum_{i=1}^{N} P_i^{зл} * C_i$$

$$C(СЗ^*) \le C_{доп};$$

При ограничениях

$$P_i^{зл} \le P_i\ доп$$

Здесь C_i - средняя величина потерь от реализации нарушителем *i*-ой цели. Складывается из потерь от нарушения конфиденциальности, от невыполнения каких-либо обязательных работ, из стоимости восстановления системы защиты при реализации злоумышленником какой-либо цели и т.п.

Сравнивая задачи 1 и 2, отметим, что они, в совокупности, близки. Задача 3 трудновыполнима в силу того, что значение C_i очень сложно определить.

Поэтому остановимся на задаче 1 и упростим ее.

Пусть есть только одна цель $Ц_i$. Существует окно опасности $t_{опас}$ – промежуток времени, когда злоумышленник «атакует». Тогда задача 1 формулируется следующим образом:

Определить такие $x_i\ (i=\overline{1,R})$ что $P_i^{ЗЛ} \to min$ при ограничениях:

$C(СЗ^*) \le C_{доп}, P_i^{зл} \le P_{iдоп}(t_{окна})$.

Решение.

Определение $P_i^{ЗЛ}$.

Рассмотрим пример. Пусть злоумышленник старается реализовать цель $Ц_1$, состоящую из трех угроз $УГ_1$, $УГ_2$, $УГ_3$, инициирую атаки в течение $t_{опас}$. За это время , возможно будет инициирован выделенный набор из трех угроз($УГ_1$, $УГ_2$, $УГ_3$) по несколько раз.

Построим граф состояния переходов (см рис. 3.3.1).

Дуги обозначаются P_{ai} / $УГ_j$ и имеют смысл вероятности перехода из состояния a_i в другое под действием j-ой угрозы. (Ждущая) вершина имеет смысл изменения вероятности нахождения в данном состоянии от последовательности однотипных угроз.

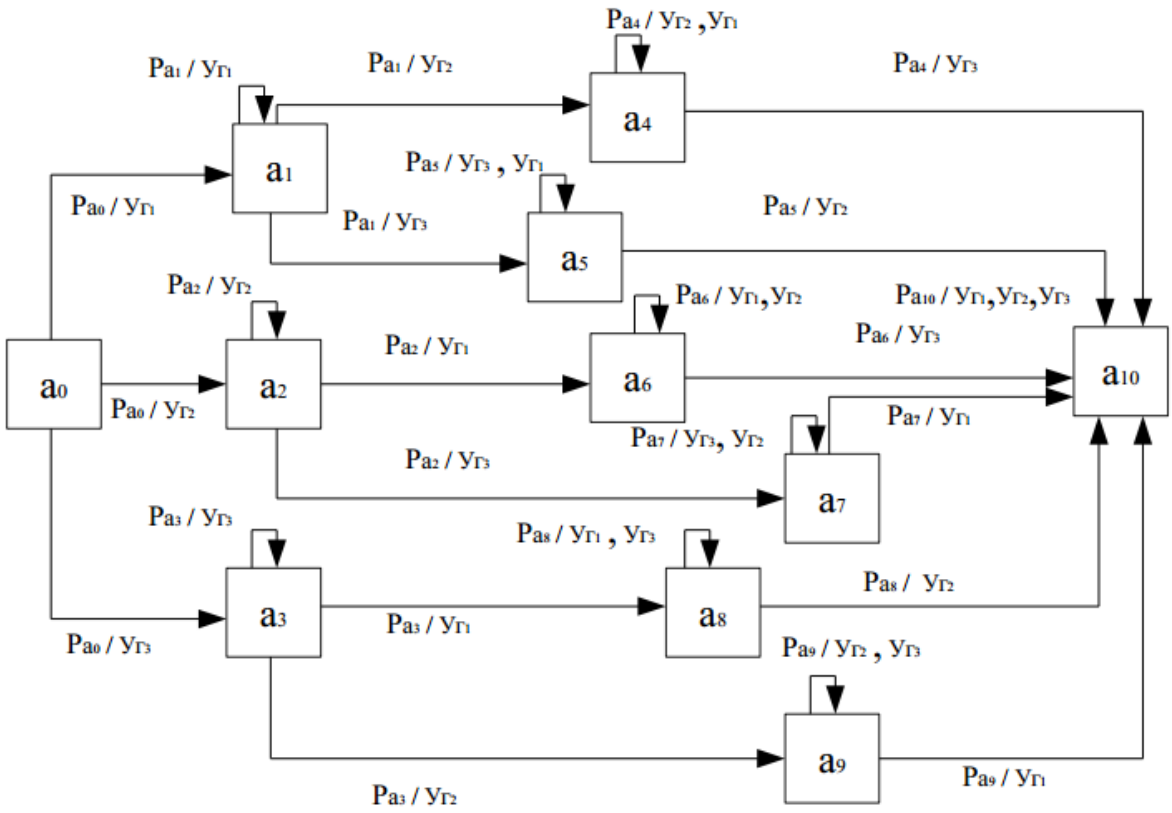


Рис.3.3.1. Определение граф $P_i^{ЗЛ}$ переходов.

Для определения P_{ai} рассмотрим типовую конструкцию (элемент) графа (см рис 3.3.2).

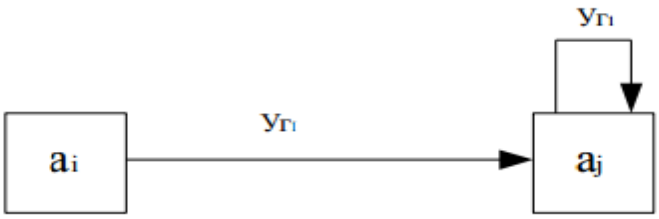


Рис.3.3.2. Типовой элемент графа переходов.

Если положить, что каждый угроза реализует различное количество раз, то аналитическая зависимость для определения $P_i^{ЗЛ}$ становится очень громоздкой. Требуются упрощения для практического применения данного подхода.

Отметим факт что атака может быть , например такой : ($УГ_1$, $УГ_2$, $УГ_3$,$УГ_1$, $УГ_2$, $УГ_3$) или такой ($УГ_1$, $УГ_1$, $УГ_2$,$УГ_2$, $УГ_3$, $УГ_3$), т.е. разной по времени возникновения угроз, роли не играет достаточно выполнить перперасчет на большее количество угроз в соответствующем состоянии (см рис 3.3.3).

Для дальнейшего рассмотрения положим , что угрозы в атаки реализуются пакетами. Для нашего примера атака выглядит следующим образом.

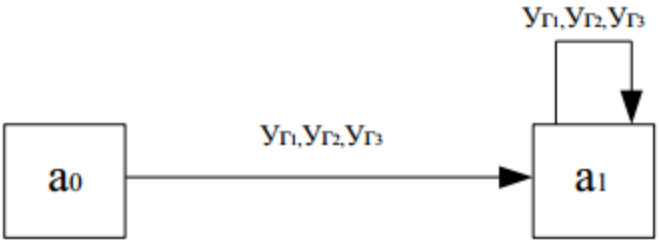


Рис.3.3.3. Упрощенный граф переходов.

С таким упрощением граф переходов будет выглядеть следующим образом (см рис 3.3.4).

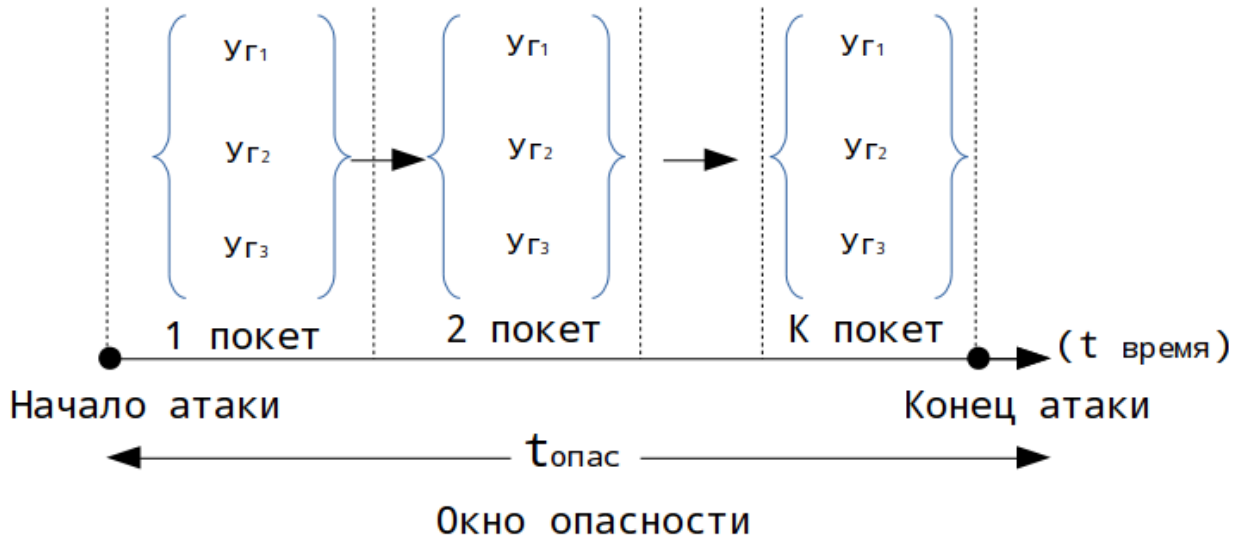


Рис.3.4.3. Атака пакетами угроз.

В данном модели $P_{a0} = 0$.

В качестве экспериментальной проверки рассмотрим подбор состава комплекса средства защиты.

В качестве защищаемой автоматизированной системы расчетов Platex - конвергентный биллинг для операторов связи (АСР), рассматривалась система низшего уровня , состоящая из рабочей станции, сервера, маршрутизаторы и аппаратуры передачи данных. Цели злоумышленника, перечень угроз информации соответствуют рассмотренным выше. Наибольшую опасность с точки зрения наносимого ущерба носят угрозы, связанные с нарушением процесса функционирования системы, что требует акцентирования большего внимания на их нейтрализацию. В качестве характеристик средств защиты, на основании осуществлялся их выбор, использовались стоимость средства и вероятность успешного функционирования по нейтрализациисоответствующей угрозы.

Моделирование проводилось для различных значений органичения на стоимость системы защиты под управлением ОС MS Windows XP, 2003-2010 на ПК.

Рассматривался подбор комплекса защитных средств, нейтрализующих все цели злоумышленника. Предположительно атака осуществляется четырехкратным повторением комплекса угроз (K =4). Время решения программы составило 30 с. Результаты моделирования представленыв таблица (3.3.1,2) и на рис. (3.3.6) и рис. (3.3.7).

Таблица 3.3.1 – Результаты моделирования подбор комплекса защитных средств, нейтрализаующих цель №3

Подбор комплекса защитных средств, нейтрализующих цель №3			
№ варианта	Номер средств защиты набора	Общая стоимость комплекса средств защиты	Вероятность достижения всех целей
1	3,4,5	1874,00	8,09E-01
2	3,5,6	1943,00	5,65E-01
3	3,5,7	2154,00	4,04E-01
4	3,6	2458,00	2,61E-01
5	3,6,7	2491,00	2,54E-01
6	3,6,8	2732,00	1,57E-01
7	3,6,9	2851,00	7,15E-02
8	3,7,8	2947,00	3,95E-02
9	3,4,7,8	3051,00	3,52E-02
10	3,5,6,7	3102,00	3,09E-02
11	3,7,8,9	3396,00	4,93E-02
12	3,4,5,7	3752,00	1,18E-02
13	3,4,6,7	4009,00	9,79E-03
14	3,4,7,8,9	4276,00	2,59E-02

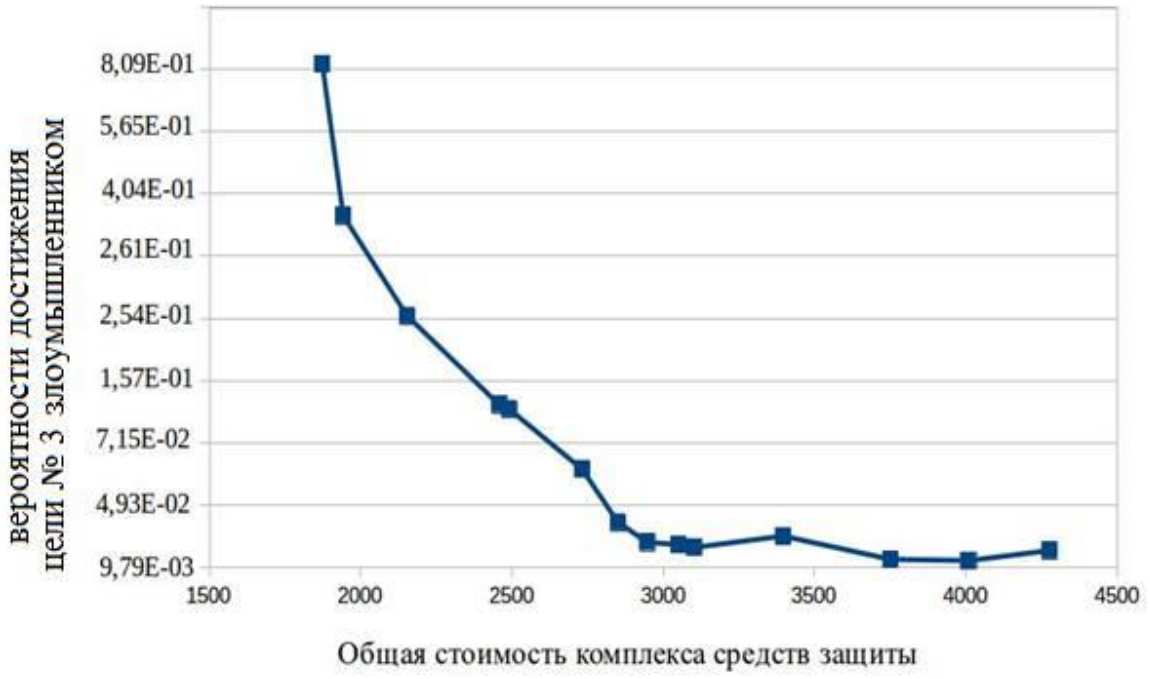


Рис. 3.3.6. Зависимость вероятности достижения цели № 3 злоумышленником от стоимости комплекса средств защиты.

Таблица 3.3.2 – Результаты моделирования подбор комплекса защитных средств, нейтрализующих всех целей.

Подбор комплекса защитных средств,нейтрализующих всех целей			
№ варианта	Номера средств защиты набора	Общая стоимость комплекса средств защиты	Вероятность реализации злоумышленником всех целей
1	1,3,4,5,7	1974,00	4,79E-02
2	1,3,5,7,8	3074,00	3,57E-02
3	1,3,5,7,9	3347,00	1,71E-02
4	1,3,5,6	3756,00	8,93E-03
5	1,3,6,7	4027,00	8,75E-03
6	1,3,6,10	4206,00	6,78E-03
7	2,3,4,5,7	4724,00	8,23E-03
8	2,3,5,7,9	4924,00	4,85E-03
9	2,3,4,8,9	5194,00	3,75E-03
10	2,6,10	5312,00	5,95E-03
11	2,3,4,6	5514,00	1,71E-03
12	3,5,6	5578,00	8,31E-04
13	3,5,7,8	5874,00	4,14E-04
14	3,4,5,7,9	6045,00	3,87E-04

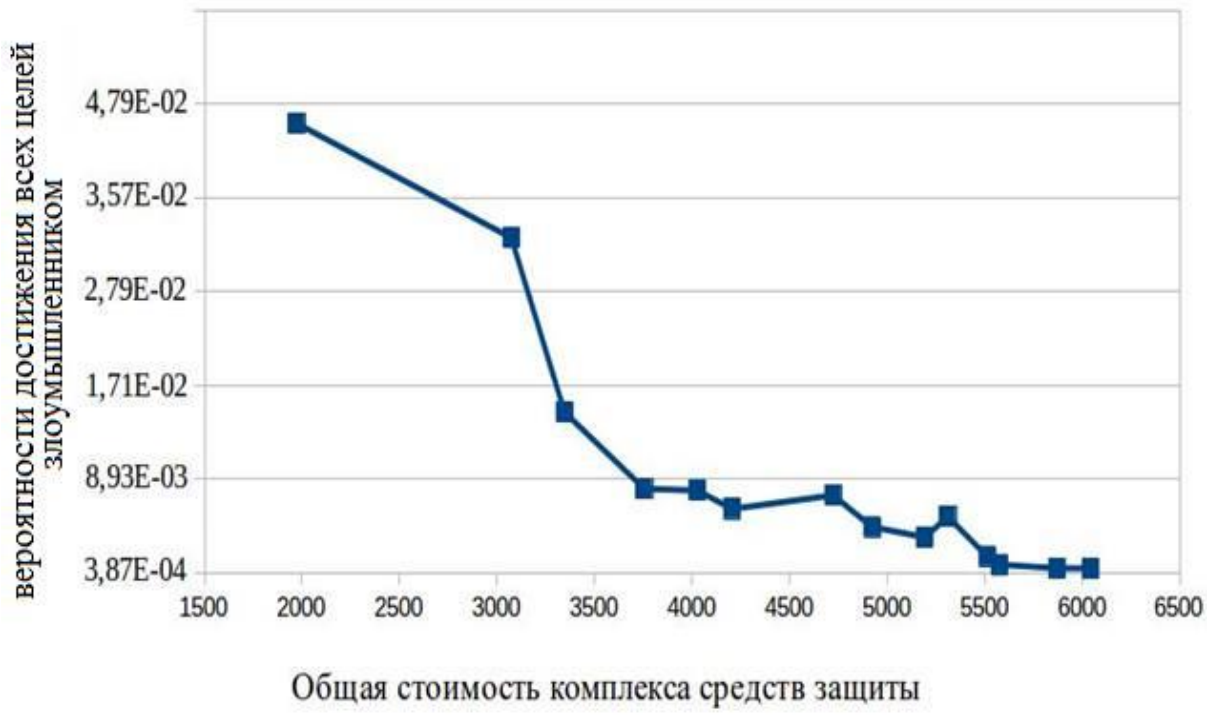


Рис.3.3.7.Зависимость вероятности достижения всех целей злоумышленником от стоимости комплекса средств защиты.

Из результатов экспериментов видно, что с увеличением объема ассигнованний на средства защиты в целом вероятность реализации злоумышленником всех целей значительно снижается. Причем, данная зависимость носит явно выраженный экспонециальный с отрицательным коэффициентом характер. Это общая тенденция. Тем не менее, в отдельных случаях стоимость средств не показатель снижения вероятность реализации злоумышленником всех целей, например , включение в состав комплекса дорогого средства защиты № 7, нейтрализующего многие из угроз, нежелательно из-за низкой эффективности блокирования этих угроз. Выигрывает , как правило, комплекс состоящий из многих недорогих средств защиты, специализирующихся на угрозах определенного вида.

Обобщенный алгоритм поиска оптимального состава СЗ, противодействующего атаке злоумышленника при реализации его конкретной цели в КИТС приведен на рис(3.3.5) и в приложения [2].

Рис.3.3.5. Схема алгоритма определение состава комплекса средств защита информации в КИТС Иордании.

3.4.Повышение отказоустойчивости транспортного уровня телекоммуникационных государтвенных сетей Иордании путём реорганизации сквозной «точка-точка» множественной адресации

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.

Транспортный уровень может выполнять сложные действия, такие, как управление потоками, коррекция ошибок и надежная доставка, необходимые порой для того, чтобы взаимодействующие приложения работали корректно и с приемлемой производительностью [79,94].

Повышения отказоустойчивости и пропускной способности в вычислительных сетях можно достичь с использованием протокола SCTP, используя параллельную передачу информации по нескольким каналам, для чего каждая ЭВМ оснащается 2 или более портами, которые подключаются в различные более простые неуправляемые или управляемые коммутаторы, создавая несколько возможных путей прохождения информации между ЭВМ.

При этом при отказе одного из каналов или коммутаторов информация, передаваемая по этому пути не теряется, а передача повторяется по оставшимся каналам, кроме того, передаваемая информация распределяется между имеющимися каналами с учетом их взаимовлияния и имеющихся потоков TCP.

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. При использовании множественных адресаций узлов SCTP могут быть организованы резервные (избыточные) соединения с ЛВС и поддерживаются различные варианты преодоления сложностей, связанных с отказами в магистральных сетях. Использование адресов с различными префиксами может обеспечить автоматическую маршрутизацию пакетов к другому оператору [2-4].

Можно использовать методы route-pinning или даже резервировать соединения с магистральными сетями, если обеспечивается контроль над сетевой архитектурой и протоколами.

Действующий вариант SCTP не поддерживает распределения нагрузки (load sharing), поэтому множественные адресации хосты обеспечивают лишь избыточность соединений для повышения уровня надежности. Один из адресов хоста указывается в качестве основного (primary) и используется как адрес получателя для всех блоков DATA при нормальной передаче. При передаче повторных блоков DATA используется один из дополнительных адресов с целью повышения вероятности доставки в конечную точку. При неоднократных повторах передачи принимается решение об отправке всех блоков DATA с использованием альтернативного адреса, пока системе мониторинга не удастся увидеть доступность основного адреса.

Для поддержки множества интерфейсов конечные точки SCTP обмениваются списками своих адресов в процессе создания ассоциации.

Каждая из конечных точек должна быть способна принимать сообщения с любого адреса, связанного с удаленным партнером; на

практике некоторые ОС могут использовать в пакетах циклический перебор адресов отправителя и в таких случаях прием пакетов с различных адресов является нормальной ситуацией. Для всего списка адресов конечной точки в данной сессии используется один номер порта [79].

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 ACK по адресу отправителя в заголовке IP блока INIT. Пример, топология сети с множественной адресацией показана на рис. 3.4.1.

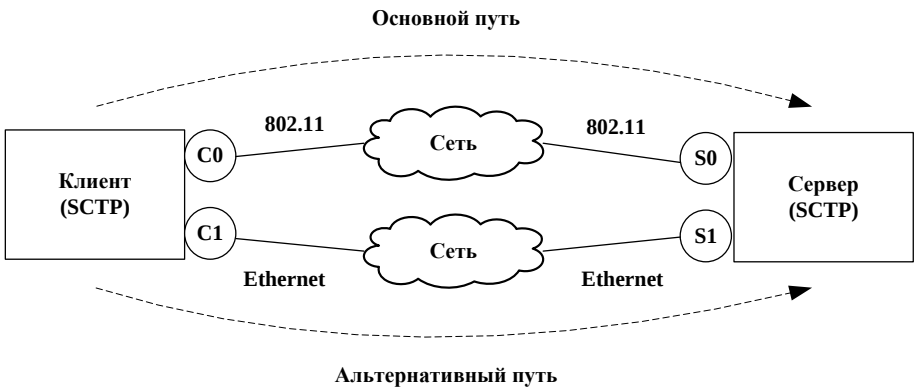


рис. 3.4.1. Топология сети с множественной адресацией

Механизм отказоустойчивости в протоколе SCTP

Каждая конечная точка использует скрытые и заданные зонды для динамической поддержки информации о достижимости IP-адресов клиентов.

Переданные данные являются скрытыми зондами для конечной точки, в то время как заданные зонды периодически тестируют достижимость и измеряют RTT (чистое время транспортировки данных от узла отправителя до узла назначения и обратно без учета времени, затраченного узлом назначения на подготовку ответа) при использовании альтернативной конечной точки.

Каждое превышение лимита времени на определенной конечной точке выдаёт количество ошибок на данном этапе, которое очищается всякий раз, когда данные, отправленные по этому назначению подтверждаются.

В случае когда количество выдаваемых ошибок превышает допустимы порог, называемый PMR (Path. Max. Retrans-Максимальное количество перезапусков), система выдаёт «отказ».

Рис.3.4.2. 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 [79].

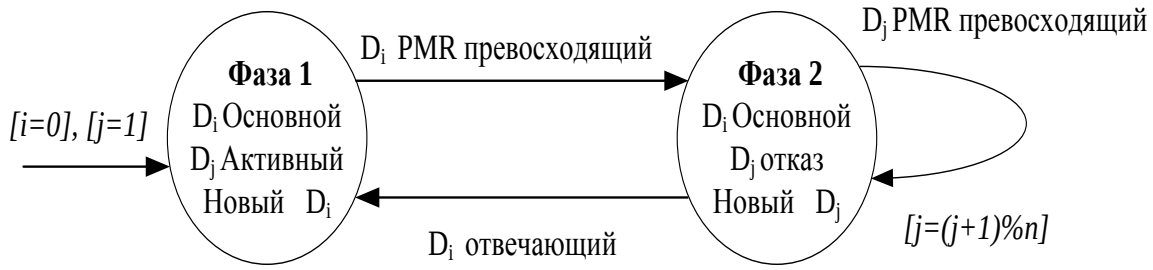


Рис 3.4.2 Автомат существующего механизма переключения.

В фазе *2* D_i остается 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.

3.5. Достоверность функционирования отказоустойчивого запоминающего устройства в корпоративных сетях Иордании при информационной защите с итеративным кодом

При использовании итеративных кодов в запоминающих устройствах телекоммуникационных сетей при их информационной защите необходимо убедиться в достоверности. Здесь приведена методика определения достоверности функционирования, которая пригодна для телекоммуникаций Иордании[98,106].

Оценку достоверности функционирования отказоустойчивых (информационно защищенных) запоминающих устройств (ЗУ) рассмотрим на примере для четырех информационных разрядов с использованием 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

$$\lambda_i = 1*10^{-9}\ \ 1/ч,\ (\ p(t) = e^{-10\ *t}).\qquad (3.5.1)$$

Вероятность безотказной работы накопителя по одному выходу равна:

$$p1(t) = p(t)^{6M}. \qquad (3.5.2)$$

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

Достоверность функционирования отказоустойчивого ЗУ оценим используя выражение:

$$D(t) = p_{ДЕК}(t)\sum_{i=0}^{k-1} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i + p_{ДЕК}(t)\sum_{i=1}^{n} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i - P_{ДЕК}(t)^2\sum_{i=0}^{k-1} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i * \sum_{i=1}^{n} C_n^i p1(t)^{(n-i)}[1-p1(t)]. \qquad (3.5.3)$$

Проведем оценку влияния кратности исправляемой ошибки аппаратурные затраты и достоверность функционирования устройств памяти при реализации предлагаемых подходов кодирования информации[98].

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 $P(t) = e^{-10^{*}t}$;

– емкость накопителя $M = 6000$;

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

Используя выражение (3.5.3) проведем сравнительную оценку достоверности функционирования (для данных из таблицы). В результате получим графические зависимости (рис 3.5.1), отображающий зависимость достоверности функционирования запоминающего устройства от времени.

Таблица 3.5.1. - Изменение кратности ошибки от 0 до5.

Контролируемый параметр	**Всего**	**Корректируемых**	**0 ош**	**1 ош.**	**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

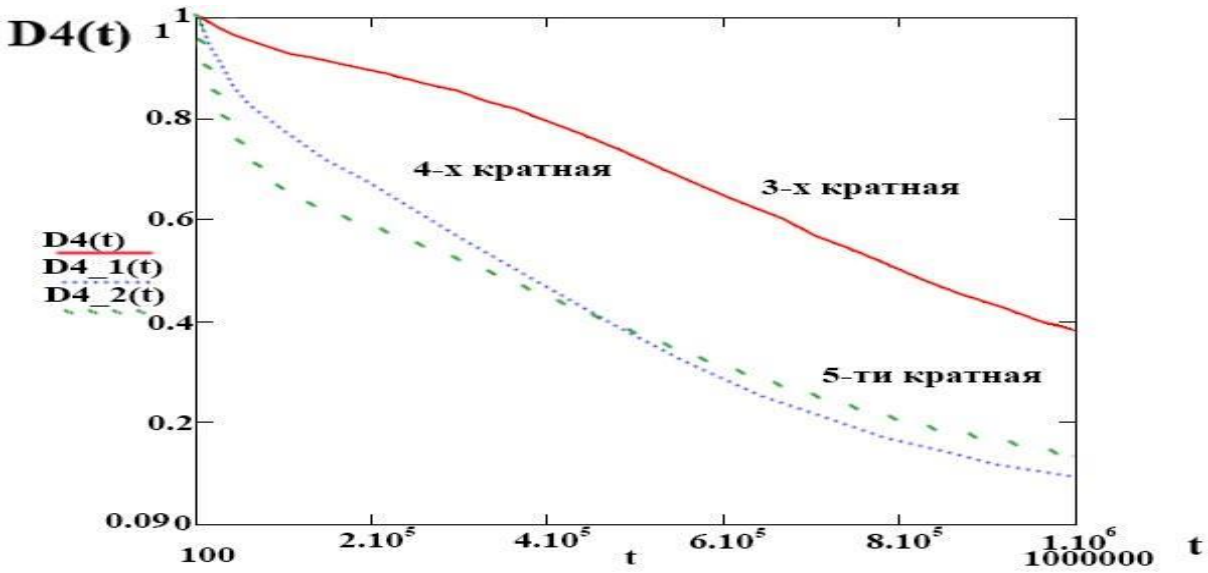


Рис.3.5.1. Сравнительная оценка достоверности функционирования от кратности исправляемой ошибки. Используя данные из таблицы рассчитаем аппаратурные затраты для построения запоминающего устройства *ca4*, сложность декодирующего устройства *cd4*, достоверность функционирования *D4*.

$$ca4 := 6M \cdot (k + 8) + k \cdot \left(-1 + \frac{l14 + l34}{2} \right) + 16 \cdot (k + 7) \cdot (l24 + l34 + l14) + l24 + 27 \cdot k + 48$$

$$ca4\_1 := 6M \cdot (k + 8) + k \cdot \left(-1 + \frac{l14\_1 + l34\_1}{2} \right) + 16 \cdot (k + 7) \cdot (l24\_1 + l34\_1 + l14\_1) + l24\_1 + 27 \cdot k + 48$$

$$ca4\_2 := 6M \cdot (k + 8) + k \cdot \left(-1 + \frac{l14\_2 + l34\_2}{2} \right) + 16 \cdot (k + 7) \cdot (l24\_2 + l34\_2 + l14\_2) + l24\_2 + 27 \cdot k + 48$$

$$cd4 := 16 \cdot (l14 + l24 + l34) \cdot (k + 7) + k \cdot \left(-1 + \frac{l14 + l34}{2} \right) + 11 \cdot k + l24 + 40$$

$$cd4\_1 := 16 \cdot (l14\_1 + l24\_1 + l34\_1) \cdot (k + 7) + k \cdot \left(-1 + \frac{l14\_1 + l34\_1}{2} \right) + 11 \cdot k + l24\_1 + 40$$

$$cd4\_2 := 16 \cdot (l14\_2 + l24\_2 + l34\_2) \cdot (k + 7) + k \cdot \left(-1 + \frac{l14\_2 + l34\_2}{2} \right) + 11 \cdot k + l24\_2 + 40$$

$$P14(t) := p(t)^{cd4} \cdot \left[\begin{array}{l} p1(t)^{16} + p1(t)^{15} \cdot (1 - p1(t)) \cdot err\_14 + p1(t)^{14} \cdot (1 - p1(t))^2 \cdot err\_24 + \\ + p1(t)^{13} \cdot (1 - p1(t))^3 \cdot err\_34 \end{array} \right]$$

$$P14\_1(t) := p(t)^{cd4\_1} \cdot \left[\begin{array}{l} p1(t)^{16} + p1(t)^{15} \cdot (1 - p1(t)) \cdot err\_14\_1 + p1(t)^{14} \cdot (1 - p1(t))^2 \cdot err\_24\_1 + \\ + p1(t)^{13} \cdot (1 - p1(t))^3 \cdot err\_34\_1 + p1(t)^{12} \cdot (1 - p1(t))^4 \cdot err\_44\_1 \end{array} \right]$$

$$P14\_2(t) := p(t)^{cd4\_2} \cdot \left[\begin{array}{l} p1(t)^{16} + p1(t)^{15} \cdot (1 - p1(t)) \cdot err\_14\_2 + p1(t)^{14} \cdot (1 - p1(t))^2 \cdot err\_24\_2 + \\ + p1(t)^{13} \cdot (1 - p1(t))^3 \cdot err\_34\_2 + p1(t)^{12} \cdot (1 - p1(t))^4 \cdot err\_44\_2 + p1(t)^{11} \cdot \\ \cdot (1 - p1(t))^5 \cdot err\_54\_2 \end{array} \right]$$

$$P24(t) := p(t)^{cd4} \cdot \sum_{i=1}^{n4} \left[\left(\frac{n4!}{i! \cdot (n4 - i)!} \right) \cdot p1(t)^{n4 - i} \cdot (1 - p1(t))^i \right]$$

$$P24\_1(t) := p(t)^{cd4\_1} \cdot \sum_{i=1}^{n4} \left[\left(\frac{n4!}{i! \cdot (n4 - i)!} \right) \cdot p1(t)^{n4 - i} \cdot (1 - p1(t))^i \right]$$

$$P24\_2(t) := p(t)^{cd4\_2} \cdot \sum_{i=1}^{n4} \left[\left(\frac{n4!}{i! \cdot (n4 - i)!} \right) \cdot p1(t)^{n4 - i} \cdot (1 - p1(t))^i \right]$$

$$D4(t) := P14(t) + P24(t) - P14(t) \cdot P24(t)$$

$$D4\_1(t) := P14\_1(t) + P24\_1(t) - P14\_1(t) \cdot P24\_1(t)$$

$$D4\_2(t) := P14\_2(t) + P24\_2(t) - P14\_2(t) \cdot P24\_2(t)$$

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

В связи с тем что в Иордании многочисленная устаревшая аппаратура, программные продукты и недостаток памяти, а необходимо вводить новую технологию для обеспечения государственных сетей, чтобы уменьшить затраты на новое оборудование используется итеративные малоразрядные коды.

Все разработанные модели и методы внедрены на предприятиях (см. Приложения 2,5,6,7).

3.6. Синтез пользовательской структуры для информационной защиты телекоммуникационных государственных сетей Иордании с маршрутизаторами с использованием САПР

В целях зашиты сети от несанкционированного доступа[64,67] 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. Для этого имеется оптимальный алгоритм для ядра в стадии преобразования маршрутизатора.

3. Генерирование маршрута и синтез топологии: Затем устройство генерирует маршруты для каждого из путей. Объединение маршрутов для всех путей завершает формирование полной топологии сети. 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[100].

4. Слияние маршрутизатора: предпоследний шаг в стадии синтеза соединяет близко находящиеся маршрутизаторы в один маршрутизатор, при условии, что ограничения длины канала передачи данных не нарушены.

5. 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 (3.6.1).

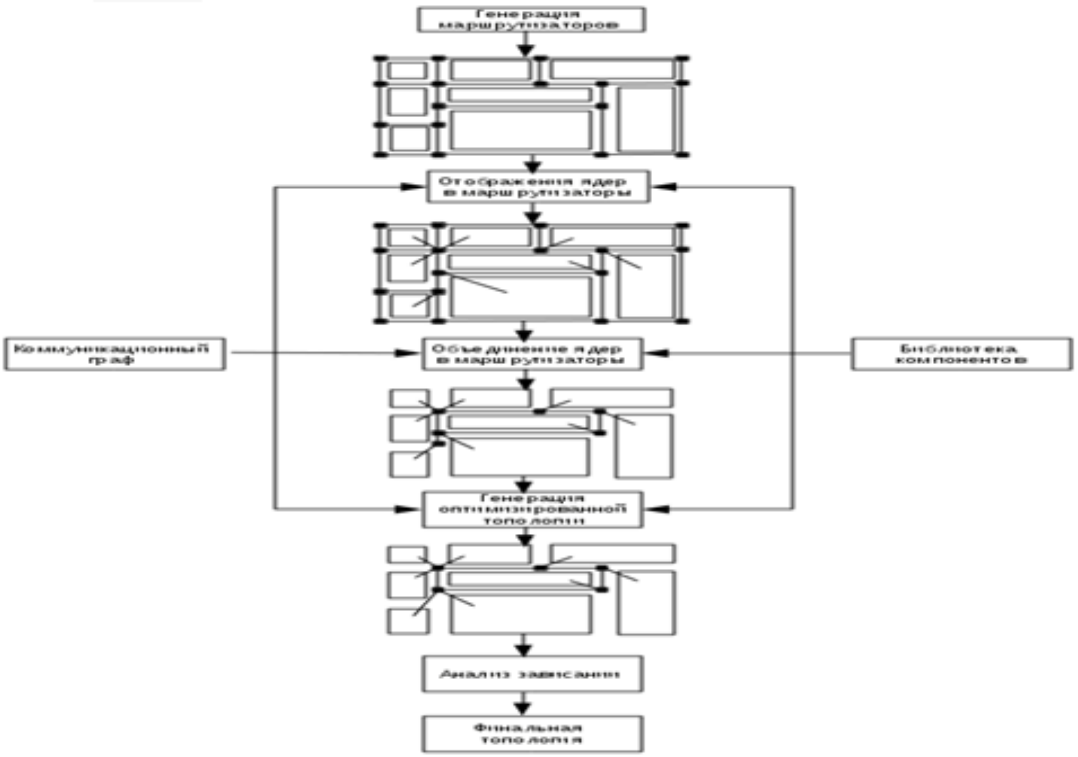


Рис.3.6.1.Схематичное проектирование специализированного приложения.

В качестве среды программирования для реализации подсистемы проектирования была выбрана система инженерных и научных вычислений MATLAB, а так же использовался язык программирования C++.

Определяющими при выборе MATLAB было:

1. Динамический обмен данными между различными приложениями на основе DDE интерфейса;

2. Встроенная реализация матричных и арифметико-логических операций над объектами произвольной размерности;

3. Использование объектно-ориентированного подхода;

4. Трансляция кода среды MATLAB в код языков программирования высокого уровня типа C, C++, FORTRAN;

5. Возможность формирования динамически подключаемых библиотек (DLL).

Система MATLAB позволяет решать многие вычислительные задачи, связанные с векторно-матричными формулировками, существенно сокращая время, которое потребовалось бы для программирования на скалярных языках (C, Pascal и т.п.). Кроме того, она предоставляет широкие возможности разработки и реализации профессиональных приложений, обеспечивает гибкую связь с другими программами.

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

1. Строку определения функции, которая задает имя, количество и порядок
2. Следования входных и выходных аргументов;
3. Первую строку комментария, которая определяет назначение функции;
4. Комментарий, определяющий спецификацию функции;
5. Тело функции - программный код, который реализует вычисления и присваивает значения выходным аргументам.

Разработанный программный комплекс представляет собой подсистему САПР, реализованную по агрегатному принципу на основе открытой архитектуры, что позволяет легко осуществлять ее наращивание.

Выбор данной концепции при создании подсистемы был сделан, исходя из критерия универсальности и легкости модификации и дополнения комплекса каждым конечным пользователем при решении своих задач.

При эксплуатации подсистемы в комплексном режиме необходимо подключение дополнительных модулей, осуществляющих импорт данных из файла отчета внешнего пакета схемотехнического моделирования. Данное обстоятельство объясняется тем фактом, что все пакеты, присутствующие на рынке САПР в настоящее время, имеют закрытую архитектуру, что делает невозможным доступ пользователя к внутренним массивам данных этих систем.

Структура комплекса представлена на рис.(3.6.2).

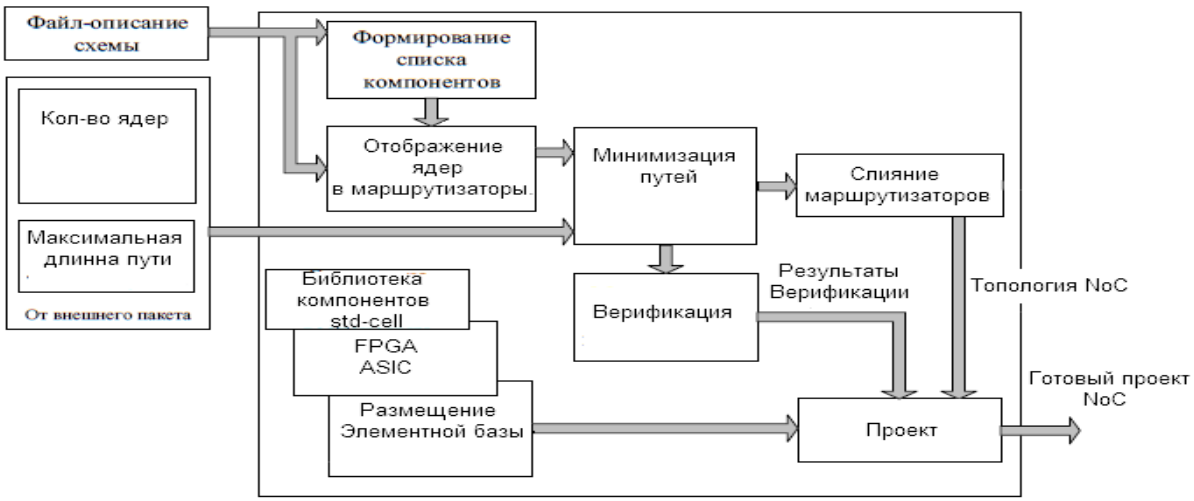


Рис.3.6.2.Структура комплекса представляет собой подсистему САПР, реализованную по агрегатному принципу на основе открытой архитектуры.

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[57,69,70].

4. Экспорт в САПР.

3.7. Выводы по главе 3

1. Проникновения в канал можно рассматривать с точки зрения теории надежности и проводить аналогии с отказами аппаратуры.
2. Найдены зависимости уровня технического состояния канала с учетом проникновений.
3. Рассчитан выигрыш во времени использования канала за счет уменьшения числа ошибок при отыскании проникновений и защите канала (в конкретных внедрениях улучшение составило 70%).
4. Для защиты каналов предприятий и учреждений Иордании необходимо оптимально выбирать определенные параметры для контроля с малоразрядными кодами с целью сокращения расходов.
5. Разработан алгоритм и программа по выбору контролируемых параметров по максимальным значениям важнейших характеристик корпоративных сетей.
6. Доказано, что использование итеративных кодов с малой разрядностью позволяет улучшить информационную защиту (достоверность) в 2-10 раз при ограниченных возможностях запоминающих устройств.
7. Разработан синтез пользовательской структуры для информационной защиты телекоммуникационных государственных сетей Иордании с маршрутизаторами с использованием САПР, что позволяет сократить время (проектирование) на 20% .
8. Разработан алгоритм определения состава комплекса средств защиты инфрмации в КИТС для Иордании.

Заключение

Диссертационная работа посвящена решению научно-технической задачи совершенствования методики защиты информации в государственных сетях Иордании с помощью малоразрядных итеративных кодов с малыми скоростями оборудования, с ограниченний ёмкостями памяти и с использованнем оригинального синтеза маршрутизоров. Для этой цели были разработаны алгоритмы и расчетные методики с обеспечением информационной безопасности государственных сетей Иордании.

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 аппаратурных 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 аппаратурные затраты более чем в 2 раза.

9. Разработан синтез пользовательской структуры для информационной защиты сети с маршрутизаторами с использованием САПР для Иордании , что позволяет сократит время (проектирование) на 20%.

10. Разработан алгоритм определения состава комплекса средств защиты инфрмации в КИТС для Иордании.

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

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

Разработанные методики и алгоритмы позволяют обеспечить комплексное решение научной задачи повышение вероятности

безотказной работы и достоверности функционнирования телекоммуникационных устройств, работающих в реальном маштабе времени для повышения информационной защищенности телекоммуникационных государственных сетей Иордании.

Библиографический список

1. Галкин А.П., Аль-Агбари Мохаммед, Аль-Муриш Мохаммед, Суслова Е.Г. Защита информации от несанкционированного доступа в системах обработки данных при физических экспериментах // Известия института инженерной физики. 2008-№ 3. - С. 2-4.

2. Галкин А.П., Дерябин А.В., Аль-Муриш Мохаммед. Нечеткий вывод, нечеткая логика и их применение при информационной защите систем // Известия института инженерной физики. 2009-№ 2. - С. 2-4.

3. Галкин А.П. и еще 9 соавторов. Методология построения комплексной системы информационной безопасности предприятия. // Монография - ред. Сухарев Е.М.- М.; Радиотехника, 2008. - 207с.: ил. – (Защита информации: кн.5)(Библиотека журнала «Радиотехника»)-ISBN 5-88070-120-4/ - С.5-70.

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

5. Суслова Е.Г., Галкин А.П. Повышение конкурентоспособности предприятия информационной защитой от несанкционированного доступа // Вестник государственного университета управления. 2010. - № 12. - С. 261-268.

6. Галкин А.П., Тахаан Осама. Угрозы информационной безопасности и защита от них для телекоммуникационных сетей радиосистем // Проектирование и технология электронных средств. 2010. № 2 . - С. 28-31.

7. 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.

8. Галкин А.П., Дерябин А.В., Аль-Муриш Мохаммед. Анализ угроз информационной безопасности в АСУТП и основные мероприятия по их

предотвращению // Известия института инженерной физики. 2009 - № 3. - С. 2-5.

9. Галкин А.П. Защита каналов связи предприятий и учреждений от несанкционированного доступа к информации: Учеб. пособие. / Владимир, Владимирский государственный университет, 2003. - 106 с.

10. Амато В. Основы организации сетей Cusco, том 1.-М.; Издательский дом “Вильямс”, 2002. - 512 с.

11. Александрович А.Е. Разработка методов и средств обеспечения и анализа надежности отказоустойчивых вычислительных систем. /Диссертация на соискание ученой степени к.т.н. 61: 96- 5/ 807-х, М.: 1994. - 163 с.

12. Барановская Т.П., Лойко В.И., Семенов М.И., Трубилин А.И. Архитектура компьютерных систем и сетей. - М.: Финансы и статистика, 2003. - 256 с.

13. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации./ Учебник для вузов. 2-е изд. - СПб.: Питер, 2006. - 703 с.

14. Бройдо В. Вычислительные системы, сети и телекоммуникации. / Учебник для вузов. 3-е изд.- СПб.: Питер, 2008. -768 с.

15. Галкин А.П. Проектирование эффективной сети связи с учетом срывов.\ Проектирование и технология электронных средств. – 2003. - № 1. - С. 9-11.

16. Денисова А., Вихарев И., Белов А., Наумов Г. Интернет. 2-е изд. – СПб. Питер. 2004. - 368 с.

17. Вентцель Е.С., Исследование операций. М.: "Советское радио", 1972.

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

19. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. - М.: Наука. Гл. ред. физ.-мат. лит. - 1987.

20. Зыль С.Н. Повышение отказоустойчивости сетевых приложений реального времени./ Сети и системы связи. 2005. - № 6. – С. 33 -37.

21. Казарин О.В., Лагутин В.С., Петраков А.В. Защита достоверных цифровых электрорадио сообщений. Учебное пособие.-М,: РИО МГУ СИ, 1997. - 68 с.

22. Дж. Уолренд. Телекоммуникационные и компьютерные сети. М.: Постмаркет. 2001. - 480 с.

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

24. Кнопелько В.К., Лосев В.В. Наднжное хранение информации в полупроводниковых запоминающих устройствах.М.:Радио и связь. 1987. - 238 с.

25. Максимов Н.В. Компьютерные сети. М.: изд. Форум, 2007. - 448 с.

26. Мырова Л.О., Чиженко А.З. Обеспечение стойкости аппаратуры связи к ионизирующим и электромагнитным излучениям. М.:Радио и связь. 1988. - 296 с.

27. Дементьев В.А., Крылов Л.Н., Осипов В.П. и др. Теория и синтез дискретных автоматов. М.: МО СССР, 1979. - 379 с.

28. Гост 27.002-89. Надежность в технике. Термины и определения. - М.: Стандарты, 1989.

29. Гост 20.911-89, Техническая диагностика. Основные термины и определения. - М.: Стандарты, 1990.

30. Дементьев В.А. Комплексное проектирование систем управления и контроля ЛА. М.: Машиностроение,1980. - 256 с.

31. Мур М., Притск Т., Риггс К., Сауфвик П. и др. Телекоммуникации. СПб.: БХВ - Петербург, 2005. - 624 с.

32. Игорь Цяпа.,Параметры производительности IIS 4/5. 2002. http://www.tsyapa.ru/tuningIIS/tuningIIS-l 1.htm (11 февраля 2004).

33. Наукова думка. Устройств с реконфигурацией структуры. Киев,1979. - 154 с.
34. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. СПб. Питер, 2004. - 864 с.
35. Карасик А.А. Математическая модель электронного конспекта лекций как компонента электронного учебного курса // Телематика-2003: Труды X всерос. науч.-метод. конф. СПб., 2003. - С. 334-335.
36. Пархоменко П.П. Основы технической диагностики. Кн. 1.-М.: Энергия, 1976. - 464 с.
37. Петраков А.В. Основы практической защиты информации М.: Радио и связь, 1999. - 368 с.
38. Половко А.М. Основы теории надежности. М.: Наука, 1964. - 356 с.
39. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы сети и телекоммуникации. / Учебник для ВУЗов. М.; Финансы и статистика, 2003. - 560 с.
40. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях, - М.:Радио и связь,1999. - 328 с.
41. Руководство по поиску неисправностей в объединенных сетях Cusco Systems. М.: Издательский дом “Вильямс”, 2003. - 1040 с.
42. Руководящий документ Гостехкоммиссии России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от не-санкционированного доступа к информации. Термины и определения. М.: Военное издательство, 1992.
43. Суворов А.Б. Телекоммуникационные системы, компьютерные сети и Интернет./Учебное пособие для вузов. М.: Феникс, 2007. - 384 с.
44. Гриценко В.И., А.М. Довгялло, А.Я. Савельева.Компьютерная технология обучения: Словарь-справочник / Под ред. Киев, 1992.

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

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

47. Хорев А.А. Способы и средства защиты информации.- М.: МО РФ, 2001. - 316с.

48. Галкин А.П., Аль-Муриш Мохаммед, Тахаан Осама. Обнаружения атак и нарушений в корпоративной сети. / Экономические проблемы ресурсного обеспечения инновационного развития региона. Матер.междунар. научн. конф. Владимир, 2009. - С.15-19.

49. Галкин А.П., Аркадьева М.С., Тахаан Осама. Кризис, безработица и информационная безопасность предприятия./ Экономические проблемы ресурсного обеспечения инновационного развития региона. Матер.междунар. научн. конф. Владимир, 2009. - С.20-24.

50. 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.

51. Галкин А.П., Тахаан Осама. Информационная защита корпоративной сети системой обнаружением атак с нечеткой логикой. / Известия института инженерной физики. 2009. - № 4. - С. 2-4.

52. Галкин А.П., Тахаан Осама. Выбор комплекса защиты информации для корпоративных информационно-телекоммуникационных сетей. / Известия института инженерной физики. 2010. - № 2. - С. 2-6.

53. Павлов А.А., Гориш А.В., Милов Ю.Г. Метод защиты памяти ЭВМ на основе корректирующих кодов с апостериорной коррекцией ошибок //

Экология, мониторинг и рациональное природопользование. Научн. тр. Вып. 302(11)-М.: МГУЛеса, 1999. - С. 259-264.

54. Петров Б.М. Рассмотрение основных показателей радиационной стойкости, позволяющих анализировать безотказность микропроцессорных и транспьютеоных устройств при радиационном воздействии // Сборник докладов международной НТК “Актуальные проблемы анализа и обеспечения надежности и качества приборов, устройств и систем”, Пенза, 1998. - С. 325-327.

55. Мамаев Е. Шкарина Л. Microsoft SQL Server для профессионалов. — СПб: Питер, 2001. - 1088 с: ил.

56. 0брайен Т., Подж С. Уайт Дж. Microsoft Access 97: разработка приложений: пер. с англ. - СПб.: БХВ - СПб., 1999. - 640 с: ил.

57. Мансуров Т.М. Отказоустойчивое функционирование управляющих устройств цифровых систем коммутации // Электросвязь, - № 9, 2000г. - С. 22-24.

58. Мельников Д.А. Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели М: КУДИЦ-ОБРАЗ, 1999. – 256 с., ил. - (Библиотека профессионала).

59. Метёлкин А.С. Архитектура программного обеспечения современных ведомственных АТС // Методы и устройства передачи и обработки информации: Межвуз. сб. науч. тр. Вып.4 / Под ред. В.В.Ромашова, В.В. Булкина. - СПб: Гидрометеоиздат, 2004. - С. 269-274.

60. Метёлкин А.С. Классификация методов коммутации в ведомственных сетях связи // Методы и устройства передачи и обработки информации: Межвуз. сб. науч. тр. Вып.4 / Под ред. В.В.Ромашова, В.В. Булкина. -СПб: Гидрометеоиздат, 2004. - С. 275-281.

61. Метёлкин А.С. Программное обеспечение цифровых коммутационных узлов командно-диспетчерских и телефонных систем связи // XXX Га-

гаринские чтения: Тез докл. Всероссийской молодежной науч. конф. - М.: МАТИ РГТУ им. К.Э. Циолковского. 2004. - С. 44.

62. Рогов С., Намиот Д. Тестирование производительности Web-серверов.Сибинфоцентр.http://www.sibinfo.ru/news/03_0l_08/server_testi ng.shtm (17 июня 2003).

63. Кириллов В.И. Многоканальные системы передачи М.: Новое знание, 2002, пер., - 752 с.

64. Гребешков А.Ю, Карташевский В.Г, Хмельницкий Д.В Анализ методов и алгоритмов сетевой маршрутизации с обеспечением QoS // Сборник докладов 57-й Научной сессии РНТО им. А.С. Попова, поев. Дню радио, 15-16.05.2002. г. Москва.

65. Ехриель И.М. Оценка задержки установления соединений в цифровой сети с интеграцией служб // Электросвязь, №7, 1993г. - С. 7-9.

66. Галкин А.П. Радиосистемы для защиты каналов связи от несанкционированного доступа к информации: Учеб. пособие / Владим. гос. ун-т. Владимир, 2003. - 104 с.

67. Кульгин М. В. Коммутация и маршрутизация IP/IPX трафика: Компьютер Пресс, 1998. – 320 с. - ил.

68. Кучерявый А.Е. Функциональная архитектура систем коммутации 90-х годов // Электросвязь, - № 9, 1996. - С. 35-37.

69. Лазарев В.Г., Гончаров Е.В. Метод динамической маршрутизации в У-ЦСИО// Электросвязь. 1999. - Ж7. – С. 34-36.

70. 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.

71. Ландэ Дмитрий. E-Government лозунг или технология? // Информационный центр ElVisti. -www.visti.net, 11.06.2003.

72. Грачев М.Н. Компьютерные технологии в прикладных политологическихисследованиях//Программы дисциплин магистерской

подготовки понаправлению социально-экономические знания / Отв. ред.: д.ф.н., проф. Зыбайлов Л.К. М.: Прометей, 1999. - С. 15-17.

73. Программы информатизации и электронное правительство//Материалы Всероссийской конференции руководителей служб информатизации. - cio.neweco.ru, 2003.

74. Юрасов. А. В. Основы электронной коммерции. Учебник для вузов.- М.:Горячая линия-Телеком, 2008. - 480с.

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

76. Ховард М., Леви М., Вэймир Р. Разработка защищенных Web-приложений на платформе Microsoft Windows 2000. Мастер-класс. / Пер. с англ. — СПб.:Питер; М.: Издательско-торговый дом «Русская Редакция», 2001. - 464 с.

77. LaVigne Mark. Electronic Government: A Vision of the Future that is Already Here//Syracuse Law Review. 2002. - Volume 52. - Number 4.

78. Черняк Л. Снова о тестах TPC. // Открытые Системы, 2000. - № 11.

79. Галкин А.П., Тахаан Осама. Повышение отказоустойчивости транспортного уровня вычислительных сетей путём реорганизации сквозной «точка-точка» множественной адресации. // Известия института инженерной физики. 2011. № 2. - С. 24-27.

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

81. Bork A. Learning with personal computers. Cambridge: Harper and Row, 1987. - 238 p.

82. Etienne Wenger. Artificial Intelligence and Tutoring Systems (Computational

and Cognitive Approaches to the Communication of Knowledge) // Morgan Kaufmann Publishers. - Los Altos, California, USA, 1987. - 487 p.
83. Hebenstreit J. Computers in education - The next step. // Education and Computing, v.l, 1995. - p. 37-43.
84. Самофалов К.Г., Корнейчук В.И., Городний А.В. Структурно-логические методы повышения надежности запоминающих устройств. М.: Машиностроение, 1976. - 350 с.
85. 1nternet Information Server 4.0: Пер. с англ. - К.: Издательская группа BHV, 1998. - 624 с.
86. Open STA Documentation. Open System Testing Architecture Organization, www.opensta.org/docs/index.html (17 июня 2003).
87. Siegfried Goschl, Microsoft Web Applications Stress Tool. JUGAT Meeting, 12 June 2001, www.javausergroup.at/events/was.pdf (17 июня 2003)
88. WebBench 4.1 Overview. eTestingLabs, 2001.
www.etestinglabs.com/benchmarks/webbench/home.asp (17 июня 2003)
89. WebStone 2.x Benchmark Description. Mindcraft, 1998,
www.mindcraft.com/webstone/ws201-descr.html (17 июня 2003) 90.XHTML 1.1 - Module-based XHTML. W3C Recommendation. 31 May 2001.
http://www.w3.org/TR/2001/REC-xhtmlll-20010531 (17 июня 2003).
90. Галкин А.П., Аркадьева М.С. Анализ экономической безопасности предприятия и некоторые мероприятия по ее улучшению // Вестник государственного университета управления. 2008. - № 8. - С.162-166.
91. Бадван Ахмед. Улучшение отказоустойчивости вычислительных сетей при множественной адресации / Тахаан О., Галкин А.П., Яремченко С.В. // Известия института инженерной физики.2012. - № 3. - С. 22-24.
92. Http://www.mir-geo.ru/vse-stran/i/telek/tele-sist.
93. Бадван Ахмед. Защита от угроз информационной безопасности в телекоммуникационных сетях / Тахаан О., Галкин А.П.// Перспективные

технологии в средствах передачи информации / Материалы 9-й Межд. научно-технической конф. Владимир-Суздаль, 2011, т.1. - С.42-45.

94. Бадван Ахмед. Улучшение экономических характеристик при повышении отказоустойчивости транспортного уровня вычислительных сетей / Тахаан О., Галкин А.П, Кирсенко И.Н.// Факторы развития региональных рынков / Материалы международной научн.- практич. конф., Владимир, 2011. - С. 23-26.

95. Бадван Ахмед. Когнитивное радио-важное направление в инновационном развитии здравоохранении / Галкин А.П., 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.

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

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

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

99. Бадван Ахмед. Минимизация при обеспечении информационной защиты в сетях / Галкин А.П., Али Альджарадат М,М,. Дарахма И,. Яремченко С.В.// Известия института инженерной физики.2013. - № 1. - С. 2-4.

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

101. Al-Jaghoub, S, Al-Yaseen, H and Al-Hourani, M. (2010). Evaluation of Awareness and Acceptability of Using e- Government Services in Developing Countries: the Case of Jordan. The Electronic Journal Information Systems Evaluation, 13(1), - C. 1-8.

102. Al-Jaghoub, S. and Westrup, C (2003). Jordan and ICT Led Development: Towards a competition State. Information Technology and People, 16(1), - C. 93-110. http://dx.doi.org/10.1108/09593840310463032 .

103. Alomari, H. (2006). E-Government Architecture in Jordan: A Comparative Analysis. Journal of Computer Science, 2(11), - C. 846-852.

104. Alomari, M, Woods, P and Sandhu, K. (2012). Predictions for e-Government Adoption in Jordan. Information Technology & People, 25(2), - C. 207-234.

105. Al-Sobhi, F., Weerakkody, V. and Al-Shafi, S. (2010). The Role of Intermediaries in Facilitating E-Government Diffusion in Saudi Arabia. Proceedings of the E uropean and Mediterranean Conference on Information Systems, pp. – C. 1-17.

106. Armstrong, C.P. and Sambamurthy, V. (1999). Information technology assimilation in firms: The influence of senior leadership and IT infrastructures. Information Systems Research, 10(4), - C. 304-327. http://dx.doi.org/10.1287/isre.10.4.304.

107. Bonham, M., Seifert, J. and Thorson, S.(2001). The transformational potential of e-government: the role of political leadership. paper presented at the panel on electronic governance and information policy (Panel 9-1) at the 4th Pan-European International Relations Conference of the European Consortium for Political Research, held at the University of Kent at Canterbury, Kent, September 9.

108. Ebrahim, Z and Irani, Z. (2005). E-government adoption: architecture and barriers. Business Process Management Journal, 11, - C. 589-611. http://dx.doi.org/10.1108/14637150510619902.

109. Edwin, L. (2003). Challenges For e-Government Development. 5th Global Forum on Reinventing Government, Mexico City, 5 November 2003.

110. Elsheikh, Y, Cullen, A and Hobbs, D. (2008). e-Government in Jordan: Challenges and Opportunities. Transforming Government: People, Process and Policy, 2(2), - C. 83-103.

111. Eman, N and Mohammad H. (2009).Computerization and e-Government implementation in Jordan: Challenges, obstacles and successes. Government Information Quarterly, 26, - C. 577-583. http://dx.doi.org/10.1016/j.giq. 2009.04.003.

112. Heba, M. Tamara, M and Amer, A. (2009). E-Government in Jordan. working paper, European Journal of Scientific Research, 35(2), - C. 188-197. http://go.worldbank.org/M1JHE0Z280 (accessed on August 10, 2012).

113. Ministry of Information and Communications Technology. Jordan e-Government Program, e-Government Strategy Report. Amman. 2012.

114. Mata, F., Fuerst, W. and Barney, J. (1995). Information technology and sustained competitive advantage: A resource-based analysis. MIS Quarterly, 19(4), - C. 487–505. http://dx.doi.org/10.2307/249630 .

115. Nasim, Q and Hafez, K. (2010). e-Government Challenges in Public Sector: A case study of Pakistan", International Journal of Computer Science Issues, 7(5), - C. 310-317. National ICT Strategy of Jordan 2007-2011.

116. Электронное правительство России на перепутье. Владимир Дрожжинов// “Центр компетенции по электронному правительству” 2013.
117. Галкин А.П. Информационная безопасность и целесообразные пути её улучшения// Palmarium Academic Publishing . Saarbruken,Deuchland, 2014. - 75 с.
118. 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.

ПРИЛОЖЕНИЕ 1

Информационная безопасность и риски при проектировании корпоративных сетей

Управление рисками становится, по сути, повседневной деятельностью для многих участников ИТ-проекта правительственных корпоративных сетей с мало разрядные коды. Вместе с тем классификация рисков и соответственно оценка значимости каждой из категорий рисков в контексте конкретного проекта - это работы, выполняемые на предпроектной стадии[2,3].

Таблица 1.2.1. Пример классификации рисков для рассмотрения сетей.

Классификация рисков	**Характеристика рисков**	**Примеры рисков**
Внутренние риски		
Проектные	Риски возникновения ошибок в проектных разработках, проектной документации, несанкционированный доступ к информации	В проектную документацию закралась ошибка, которая выявилась только на поздней стадии проекта. Результат - перерасход средств и увеличение сроков выполнения проекта
Технические	Риски неправильных технических решений и неправильного использования технических устройств, несанкционированный доступ к информации	Приобретенное по лизингу оборудование оказалось ненадежным и постоянно отказывает в работе. Результат - простои в работе, увеличение сроков проекта, затраты на ремонт оборудования
Технологические	Риски применения непроверенных технологий и методик, несоблюдения установленных норм и правил,	В результате того, что методология выполнения проекта не предусматривала подготовку и утверждение документа "Отчет о

	несанкционированный доступ к информации	предпроектном обследовании", возникли разногласия в ходе согласования технического проекта
Организационные	Риски возникновения ошибки планирования, неэффективной координации работ, несанкционированный доступ к информации и т. п.	При формировании команды проекта не был назначен ответственный за контроль качества. В результате проект выполнен с большими претензиями со стороны заказчика
Финансовые	Риски перерасхода бюджета проекта из-за неправильных оценок, срывов сроков выполнения работ, ошибок исполнителя и т. п.	При оценке бюджета проекта не было четко определено распределение обязанностей заказчика и исполнителя. В результате проект выполнен с превышением бюджета в несколько раз
Внешние риски		
Природные	Риски, связанные с природными или социальными явлениями (форс-мажор)	В сервер БД ударила молния
Политические	Риски, связанные с нестабильностью деятельности органов власти, несанкционированный доступ к информации	Неожиданные государственные меры регулирования в сферах ценообразования, налогообложения, проектных нормативов и т. п.
Социальные	Риски, связанные с разделением интересов разных социальных групп и ростом	Вандализм, саботаж, забастовки и пр.

	социальной активности населения	
Экономические	Риски, связанные с экономической политикой государства; финансовые риски, связанные с кризисом денежно-кредитной системы, инфляцией; валютные риски, связанные с изменением курсов валют	В результате дефолта 1998 г. многие проекты были закрыты или приостановлены
Экономические		Управлять такими рисками можно только на макроуровне, а на уровне проекта эти риски необходимо анализировать и учитывать, чтобы минимизировать возможный ущерб от их наступления

ПРИЛОЖЕНИЕ 2

Инфраструктура государственных сетей Иордании.

Системный проект предназначен для создания на его основе государственной Программы «Информационное общество», уточнения содержания иных программ, находящиеся на данный момент в стадии выполнения или разработки.

Это являются конкретизацией положений Концепции формирования государственных сетей в Иордании до 2016 г., одобренной распоряжением государства Иордании от 2004 г.[103].

Главной целью формирования государственного сетей является повышение качества государственного управления, которое выражается через:

1.Снижение временных, организационных и финансовых издержек для граждан и организаций при получении государственных (муниципальных) услуг;

2.Снижение административных барьеров и бремени избыточного регулирования для хозяйствующих субъектов;

3.Сокращение бюджетных расходов на деятельность органов исполнительной власти и повышение эффективности этих расходов;

4.Повышение прозрачности деятельности органов государственной власти.

Для построения информационного общества необходимы максимально широкие преобразования, затрагивающие все ветви и уровни государственной власти и местного самоуправления, сферы общественных отношений (здравоохранение, образование, культура и т.д.), бизнес и граждан. Формирование государственных сетей подразумевает решение меньшего круга задач, связанных лишь с исполнительной, законодательной и судебной ветвями власти.

В актах государства Иордании, принятых в 2008–2010г. немалое внимание уделено вопросам государственного управления и административной эффективности (в противовес экстенсивной информатизации), что позволило инициировать формирование отдельных компонентов государстваенных сетей (таких как создание реестра и портала государственных услуг, системы межведомственного электронного взаимодействия и др.)[103,111].

Государственные сети - такие системы документооборота государственных управления, которая основана на автоматизации всей совокупности управленческих процессов в масштабах страны и служат для определенной цели: существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества.

Создание государственных сетей предполагает построение общегосударственные распределенные системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки.[105].

Государственные сети имеет несколько видов взаимодействия:

- между государством и гражданами (G2C, Government-to-Citizen);
- между государством и бизнесом (G2B, Government-to-Business);
- между различными ветвями государственной власти (G2G, Government-to-Government);
- между государством и государственными служащими (G2E, Government-to-Employees);

В состав государственных сетей может входить:

-оптимизация предоставления государственных услуг населению и бизнесу;

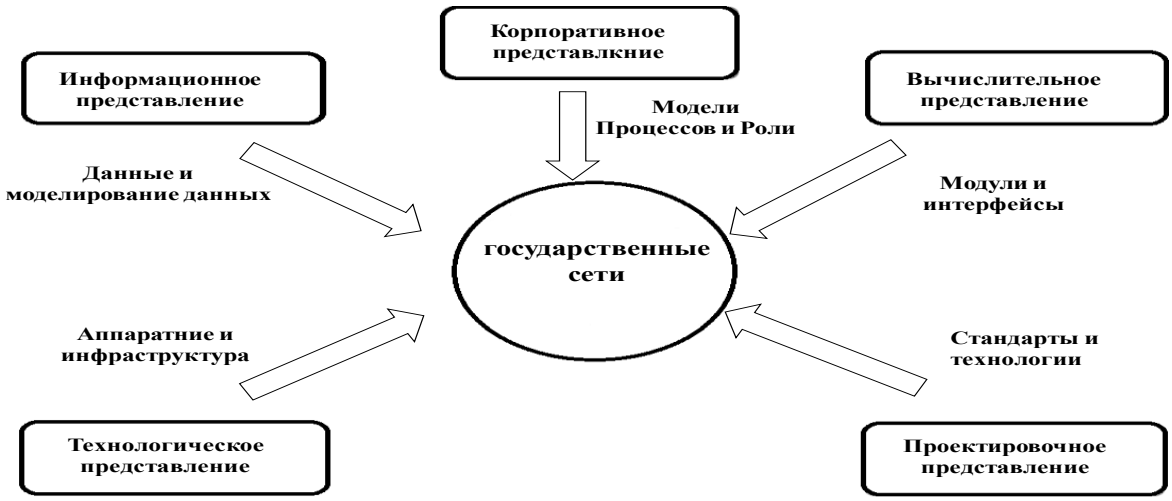
-поддержка и расширение возможностей самообслуживания граждан;

-рост технологической осведомленности и квалификации граждан;

-повышение степени участия всех избирателей в процессах руководства и управления страной;

-снижение воздействия фактора географического местоположения;

В государственных сетях, также, может обеспечивать эффективное и менее затратное администрирование; кардинальное изменение взаимоотношений между обществом и государством; совершенствование демократии и повышение ответственности власти перед народом



В условиях развития информационно-коммуникационных технологий все сферы деятельности государственных органов в электронном виде являются востребованными гражданами и организациями различных форм собственности.

Актуальность данного направления подчеркивается динамичностью развития таких сфер как, социальная, юридическая, экономическая, культурная, медицинская, муниципальная сферы и др.

Существует еще и «Проектное управление», где идет разработка, формирование, внедрение, координация и реализация проектов, стратегий, а также программ информатизации и связи в исполнительные органы государственной власти и подведомственные им организации в целях обеспечения потребности населения, государственных органов, органов местного самоуправления и.т.д. Все проектные управления имеют определенные задачи, установленные менеджерами.

Основными задачами можно считать реализацию программ развития информатизации и связи, в том числе системы «государственных сетей»; координацию и продвижение работ по внедрению новейших технологий в части информатизации и связи в исполнительных органах государственной власти; оптимизацию и регламентирование процессов планирования, контроля, корректировки планов проектов; отслеживание хода выполнения целевых программ, реализуемых Министерством; аналитику результатов и формирование отчетности по факту реализации мероприятий в области развития информатизации и связи; подготовку проектной документации для участия в конкурсах.

Государственные сети Иордании не является дополнением или аналогом традиционным сетей государства, а лишь определяет новый способ взаимодействия на основе активного использования информационно-коммуникационных технологий (ИКТ) в целях повышения эффективности предоставления государственных услуг.)[114].

Очевидно, что ГС ставит перед собой определенные задачи цели. Среди них и оптимизация предоставления государственных услуг населению и бизнесу; повышение степени участия всех избирателей в процессах руководства и управления страной; поддержка и расширение возможностей самообслуживания граждан; рост технологической осведомленности и квалификации граждан; снижение воздействия фактора географического местоположения.

Создание ГС должно обеспечить не только более эффективное и менее затратное администрирование, но и кардинальное изменение взаимоотношений между обществом и государством, что, в конечном счете может привести к совершенствованию демократии и повышению ответственности власти перед народом.

Требования, предъявляемые к инфраструктурам государственных сетей, подлежат правовому закреплению государством Иордании:

1. Общность использования:- Реализация инфраструктурной ИС должна обеспечивать взаимодействие неопределенного круга ИС, в том числе неизвестных заранее (ее реализация не должна зависеть от ИС, взаимодействие которых она обеспечивает).

2. Использование открытых стандартов: - Инфраструктура ИС должна обеспечивать доступ к предоставляемым ею сервисам посредством единообразных интерфейсов, отвечающих критериям открытых стандартов.

3. Технологическая нейтральность: - Инфраструктура ИС не должна требовать от прикладных и иных инфраструктурных ИС использования какой-либо конкретной технологии, программного обеспечения или аппаратной платформы.

4. Стабильность ИС заключается в неизменности основных характеристик, форматов, регламентов функционирования инфраструктурной ИС, которая должна обеспечиваться в течение продолжительного времени.

5. В случае модернизации ИС должна быть обеспечена продолжительная поддержка функционирования замещаемых протоколов, форматов, спецификаций, предоставление сервисов по замещаемым регламентам – в этом состоит преемственность инфраструктуры ИС.

6. Повсеместная доступность:- Инфраструктура ИС должна обеспечивать доступность своих сервисов на всей территории Иордании и — в случаях, установленных законодательством, — за ее пределами.

7.Постоянная работоспособность:- Инфраструктура ИС должна обеспечивать доступность своих сервисов круглосуточно без перерывов и отказов в обслуживании.

8. Нагрузочная способность и способность к масштабированию:- Инфраструктура ИС должна обладать достаточным запасом по пропускной способности и вычислительной нагрузке, в том числе в условиях прогнозируемых пиковых нагрузок.

Реализация стратегии формирования информационного общества (ИО) в части «государственных сетей» характеризуется рядом проблем. Их можно классифицировать следующим образом: методологические, информационные, технологические и финансовые.

Методологические проблемы охватывают вопросы методической поддержки национальной программы ускоренного развития услуг в сфере информационно-коммуникационных технологий (ИКТ) до 2016г.

В соответствии со стратегией предусматривалось научно-методологическое обеспечение: исследование социально-экономических и политических проблем развития ИО, разработка научных основ и исследование проблем управления процессом развития ИО; разработка и развитие методов и средств контроля, планирования, оценки и прогнозирования состояния, хода и результатов развития ИО и информатизации; организация проведения научных исследований и разработок в сфере ИКТ.

Необходимые условия для решения проблем подготовки госуслуг:

1.Организация единого, комплексного подхода к процессу подготовки госуслуг, с учетом всех составных компонентов, на необходимом и достаточном уровне структуризации и формализации самой услуги;

2.Применение при подготовке услуг к переводу в электронный вид промышленных технологий с использованием языков программирования, которые подразумевают манипуляции с объектами моделей данных, автоматическую интерпретацию метаданных.

3.Обеспечение коллективной работы большого количества участников в рамках семантического, нормативно-правового и организационно-методического пространства для реализации полноценного взаимодействия.

ПРИЛОЖЕНИЕ 3

Особенности государственных сетей Иордании

Существенным фактором, оказывающим значительное влияние на положение дел в информационной области вообще, и в сфере защиты информации, в частности, является то, что до начала 90-х годов нормативное регулирование в данной области оставляло желать лучшего. Некоторые ключевые для государственных сетей вопросы в данной области не решены до сих пор[50,77].

В то же время инфраструктура государственных сетей (ИГС) – это совокупность автоматизированных и телекоммуникационных систем, обслуживающих процессы информационного взаимодействия всех субъектов электронных государственных сетей, поддерживая необходимый уровень предоставления государственных услуг потребителям в электронной форме (схема № 1). Именно эта инфраструктура создается в рамках программы «Информационное общество».

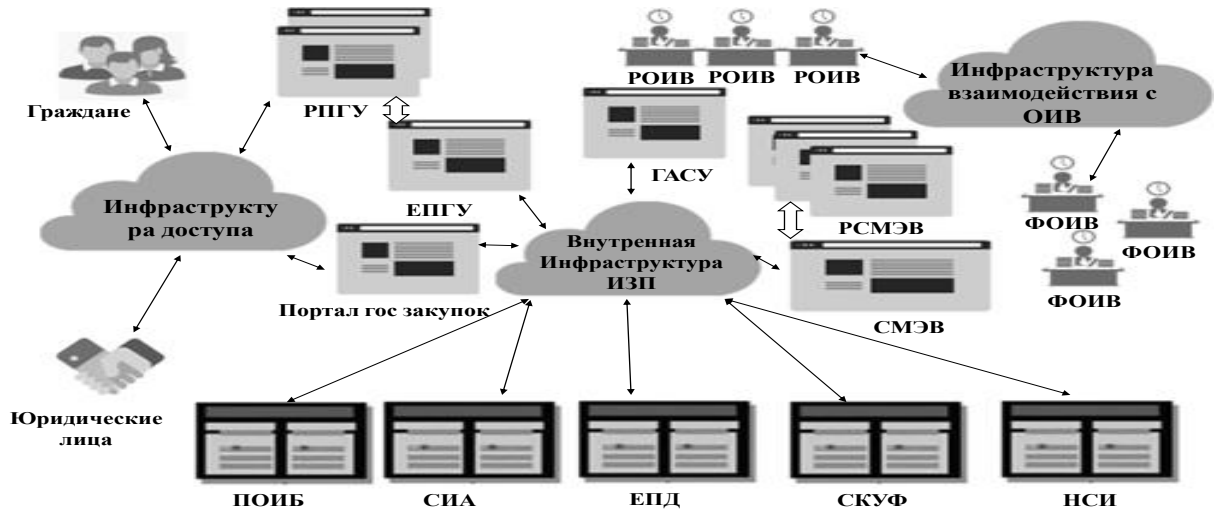


Схема 1. Архитектура инфраструктура создается в рамках программы «Информационное общество».

Принципы регулирования интерфейсов информационных систем

Обобщение мирового и отечественного опыта позволяет выделить несколько принципов, которые на современном этапе

применяются во всех странах, использующих стандартизацию интерфейсов государственных информационных систем[73,116]:

1. Принцип зрелости спецификаций и их поддержки рынком. Для реализации интерфейсов государственных информационных систем допускаются только те спецификации, которые не несут риска потери государственных инвестиций по причине бесперспективности спецификации.

2. Принцип минимума обременений. Приоритет получают те спецификации, использование которых накладывает минимум ограничений на пользователей, не принуждают их к приобретению конкретного ПО.

3. Принцип приоритетности открытых стандартов. В случаях, когда для решения определенной технологической задачи существует открытый стандарт, предпочтение должно отдаваться ему, а не нестандартной технологи.

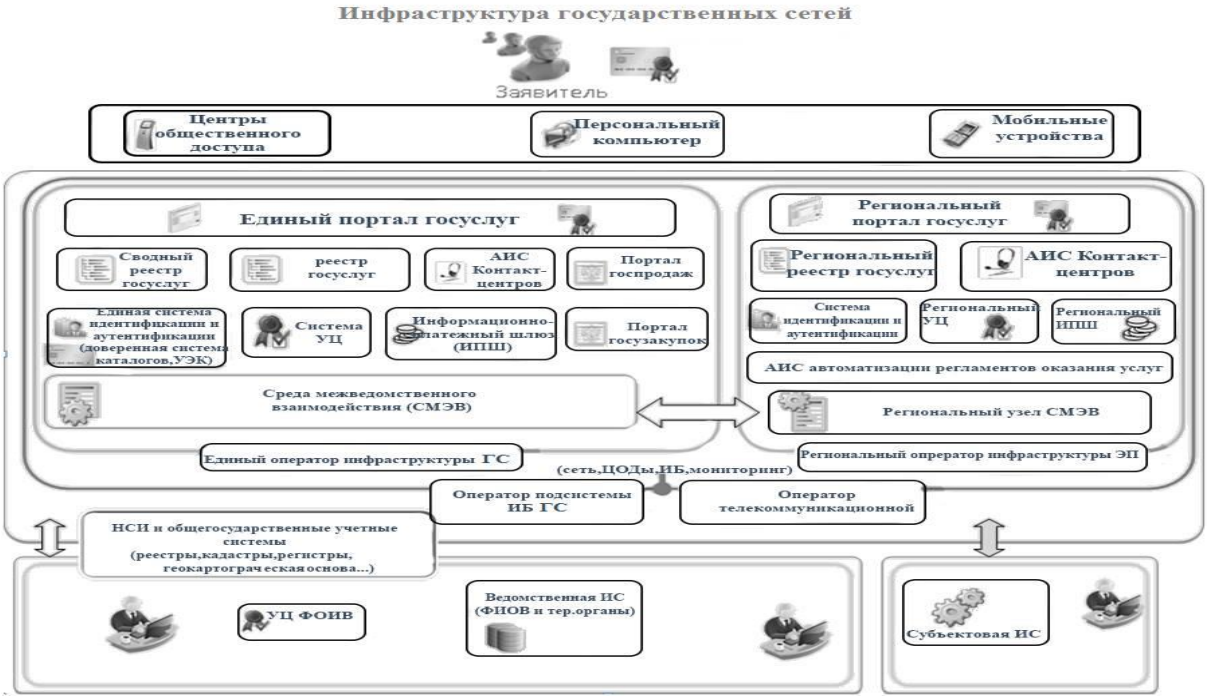


Рис.2.3.1. Ключевые компоненты инфраструктуры государственных сетей в составе региональных сегментов городах и других населеных пунктов Иордании.

Инфраструктура цифрового доверия.

Инфраструктура цифрового доверия (далее ─ ИЦД) включает в себя удостоверяющие центры, входящие в единый домен цифрового доверия, и обеспечивает единое пространство использования и признания цифровой подписи. Вместе с тем, в настоящее время в Иордании отсутствует единое национальное пространство доверия.

Существующие корпоративные, ведомственные и региональные системы не обладают признаками инфраструктурности за пределами собственного сегмента, как правило, соответствующего корпорации, отрасли, ведомства или региона. Возможная реализация инфраструктуры цифрового доверия приведена на рис 2.3.2.

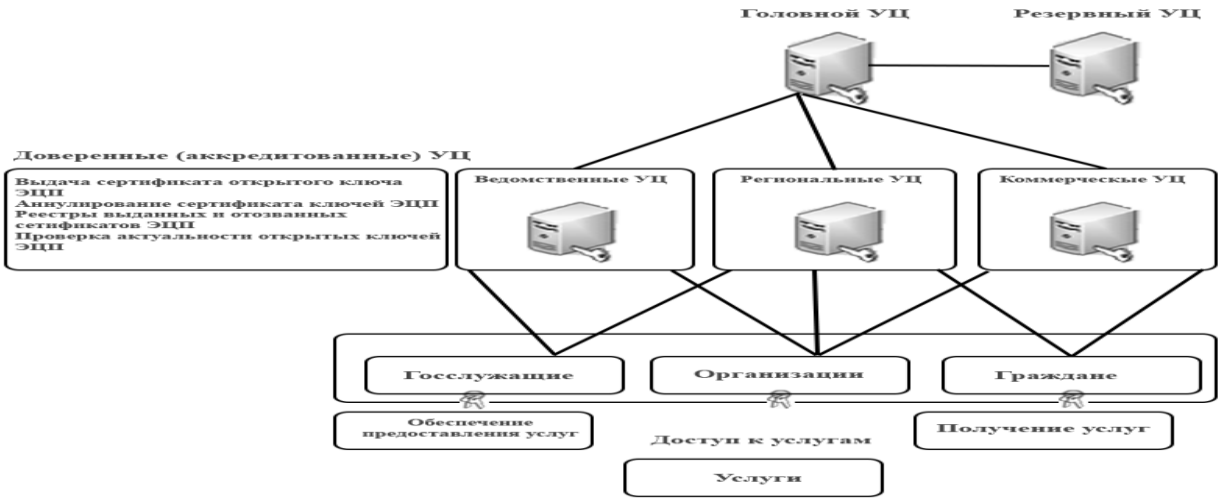


Рис 2.3.2.инфраструктуры цифрового доверия.

В 2012 г. для ЕПГУ было приобретено более 5 серверов HP, несколько маршрутизаторов Cisco и систем хранения Hitachi вместе с СУБД Oracle. Для СМЭВ использовались один блейд-сервера и ленточная библиотека Sun, сервер HP, дисковый массив Hitachi и коммутатор Brocade. В качестве программной шины было приобретено решение Oracle.

Предположим в 2016 г. вычислительные мощности расширяется. На этот раз в основном за счет оборудования IBM. Инфраструктура ЕПГУ потребляет 8 новых серверов, СМЭВ — три. Помимо этого, техника IBM с 2016 г[71,107].

ПРИЛОЖЕНИЕ 4

Некоторые алгоритмы защиты

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

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.

Тип	Описание
DES (Data Encryption Standard)	Популярный алгоритм шифрования, используемый как стандарт шифрования данных правительством США. Шифруется блок из 64 бит, используется 64-битовый ключ (требуется только 56 бит), 16 проходов. Может работать в 4 режимах: 1) Электронная кодовая книга (ECB-Electronic Code Book) - обычный DES, использует два различных алгоритма. 2) Цепочечный режим (CBC-Cipher Block Chaining), в котором шифрование блока данных зависит от результатов шифрования предыдущих блоков данных. 3) Обратная связь по выходу (OFB-Output Feedback), используется как генератор случайных чисел. Обратная связь по шифратору (CFB-Cipher Feedback), используется для получения кодов аутентификации сообщений.
3-DES или тройной DES	64-битный блочный шифратор, использует DES 3 раза с тремя различными 56-битными ключами. Достаточно стоек ко всем атакам
Каскадный 3-DES	Стандартный тройной DES, к которому добавлен механизм обратной связи, такой как CBC, OFB или CFB. Очень стоек ко всем атакам.
FEAL (быстрый	Блочный шифратор, используемый как альтернатива DES. Вскрыт,

алгоритм шифрования)	хотя после этого были предложены новые версии.
IDEA (международный алгоритм шифрования)	64-битный блочный шифратор, 128-битовый ключ, 8 проходов. Предложен недавно; хотя до сих пор не прошел полной проверки, чтобы считаться надежным, считается более лучшим, чем DES
Skipjack	Разработано АНБ в ходе проектов правительства США "Clipper" и "Capstone". До недавнего времени был секретным, но его стойкость не зависела только от того, что он был секретным. 64-битный блочный шифратор, 80-битовые ключи используются в режимах ECB, CFB, OFB или CBC, 32 прохода
RC2	64-битный блочный шифратор, ключ переменного размера. Приблизительно в 2 раза быстрее, чем DES. Может использоваться в тех же режимах, что и DES, включая тройное шифрование. Конфиденциальный алгоритм, владельцем которого является RSA Data Security
RC4	Потоковый шифр, байт-ориентированный, с ключом переменного размера. Приблизительно в 10 раз быстрее DES. Конфиденциальный алгоритм, которым владеет RSA Data Security
RC5	Имеет размер блока 32, 64 или 128 бит, ключ с длиной от 0 до 2048 бит, от 0 до 255 проходов. Быстрый блочный шифр. Алгоритм, которым владеет RSA Data Security
CAST	64-битный блочный шифратор, ключи длиной от 40 до 64 бит, 8 проходов. Неизвестно способов вскрыть его иначе как путем прямого перебора.
Blowfish.	64-битный блочный шифратор, ключ переменного размера до 448 бит, 16 проходов, на каждом проходе выполняются перестановки, зависящие от ключа, и подстановки, зависящие от ключа и данных. Быстрее, чем DES. Разработан для 32-битных машин
Устройство с одноразовыми ключами	Шифратор, который нельзя вскрыть. Ключом (который имеет ту же длину, что и шифруемые данные) являются следующие 'n' бит из массива случайно созданных бит, хранящихся в этом устройстве. У отправителя и получателя имеются одинаковые устройства. После использования биты разрушаются, и в следующий раз используются

	другие биты.
Поточные шифры	Быстрые алгоритмы симметричного шифрования, обычно оперирующие битами (а не блоками бит). Разработаны как аналог устройства с одноразовыми ключами, и хотя не являются такими же безопасными, как оно, по крайней мере практичны.

Асимметричные алгоритмы

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.

Тип	Описание
RSA	Популярный алгоритм асимметричного шифрования, стойкость которого зависит от сложности факторизации больших целых чисел.
ECC (криптосистема на основе эллиптических кривых)	Использует алгебраическую систему, которая описывается в терминах точек эллиптических кривых, для реализации асимметричного алгоритма шифрования. Является конкурентом по отношению к другим асимметричным алгоритмам шифрования, так как при эквивалентной стойкости использует ключи меньшей длины и имеет большую производительность. Современные его реализации показывают, что эта система гораздо более эффективна, чем другие системы с открытыми ключами. Его производительность приблизительно на порядок выше, чем производительность RSA, Диффи-Хеллмана и DSA.
Эль-Гамаль.	Вариант Диффи-Хеллмана, который может быть использован как для шифрования, так и для электронной подписи.

«Утверждаю»
Генеральный директор
НПО «Владремстрой»

О. Л. Смушко
15. 01 2014

АКТ ВНЕДРЕНИЯ

Результаты, полученные **Бадваном Ахмедом** (гражданином Иордании) при выполнении диссертационной работы внедрены на нашем предприятии в 2011-2014гг. в виде технико - экономического обоснования целесообразности информационной защиты; методик применения различных способов защиты информации от несанкционированного доступа; рекомендаций по защите телекоммуникационных и компьютерных сетей.

Они нашли практическое применение при обмене информацией с нашими филиалами

Указанные методики хороши тем, что при сравнительно небольших затратах обеспечивают высокую эффективность.

Начальник отдела телекоммуникаций- С.Э. Кузнецов

Начальник лаборатории - А.Г. Звягинцев

«Утверждаю»

Генеральный директор

ПФ «Электроприбор» (г. Москва)

Н. И. Захарова

4 декабря 2013 г.

Акт внедрения

Результаты, полученные **Ахмедом Бадваном** (гражданином Иордании) при выполнении диссертационной работы, внедрены на нашем предприятии в 2012-13 гг. в виде расчетных методик, в частности, с учетом экономической целесообразности защиты информации. Высокий уровень подтверждается применением солидного математического аппарата и другими разработками.

Проведена проверка на наличие возможных путей проникновения в системы связи нашего предприятия и защиты от них.

Использованы рекомендации по защите компьютерных и телекоммуникационных сетей от несанкционированного доступа к информации.

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

Ведущий инженер- **Андреев А.И.**

«Утверждаю»
Генеральный директор
НПО «РИК»,

к. т. н .-

А. В. Поляков

15.01.14

Акт внедрения

Результаты, полученные **Бадван Ахмедом** (гражданина Иордании) при выполнении диссертационной работы, в частности:

1) Методики применения различных способов защиты информации от несанкционированного доступа;

2) Рекомендации по защите телекоммуникационных и компьютерных сетей;

3) Технико –экономическое обоснование целесообразности информационной защиты;

внедрены на нашем предприятии в 2012-2014гг. Они нашли практическое применение при обмене информацией с нашими филиалами в гг. Иваново, Санкт-Петербург, Омске и т.п.

Указанные методики хороши тем, что при сравнительно небольших затратах обеспечивают высокую эффективность и не требуют специальной подготовки нашего персонала.

Начальник отдела корпоративной телекоммуникации- Сирко С. Э.

Начальник лаборатории связи - Сергеев А.Г.