МИНИСТЕРСТВО ОБРАЗОВАНИИ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных систем и Геотехнологий

ВЫПУСКНАЯ ДИПЛОМНАЯ РАБОТА

На тему «Разработка динамической модели управления безопасностью локальной вычислительной сети»

Исполнитель Минкин Павел Андреевич

(фамилия, имя, отчество)

Руководитель Доктор техн. наук, профессор

(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич

(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____

(подпись)

Доктор техн. наук, профессор

(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич

(фамилия, имя, отчество)

“17” февраля **2017г.**

Санкт-Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИИ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных систем и Геотехнологий

ВЫПУСКНАЯ ДИПЛОМНАЯ РАБОТА

На тему «Разработка динамической модели управления безопасностью локальной вычислительной сети»

Исполнитель Минкин Павел Андреевич

(фамилия, имя, отчество)

Руководитель Доктор техн. наук, профессор

(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич

(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____

(подпись)

Доктор техн. наук, профессор

(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич

(фамилия, имя, отчество)

“___”_____2017г.

Санкт-Петербург

2017

Содержание работы

1.Введение

1.1. Актуальность рассматриваемого процесса.

Информационные технологии включают в себя различные аспекты работы с информацией: сбор, обработку, преобразование, хранение и распределение или передачу. До прихода ИТ в повседневную жизнь в мире использовался и развивался формат физических бумажных носителей, которые имели в своей основе символы (буквы или цифры).

В настоящее время информационно-деловая активность человечества смещается и переходит из области физической обработки информации в цифровую. Безусловно, преймуществами такого способа является ускорение и удешевление рутинных процессов, что в современных реалиях дает большое преймущество во времени, а время есть важнейший ресурс. Обмен информацией в электронном виде быстрее, дешевле и надежнее бумажного- электронное письмо, к примеру, доходит за считанные мгновения, в отличие от «бумажного». Пока бумажное письмо дойдет до адресата, информация, хранящаяся в нем может стать неактуальной. В то время как передачей писем через почтовое отделение занимается отдельная организация, передача электронного письма осуществляется через канал, который может использоваться для решения целого спектра задач: от просмотра видеороликов в сети Интернет, до мониторинга курса валют в реальном времени.

Данные процессы играют ключевую роль в современном мире, поэтому стоит уделить соответствующее внимание обеспечению информационной безопасности информации. Информационные ресурсы предприятия, государства или отдельного человека могут представлять ценность, и их несанкционированное использование нередко может принести ущерб. Любая информационная система может состоять из множества взаимосвязанных компонентов, нарушение работы которых

может привести к сбою в работе всей системы. Будь то государственная тайна, или конфиденциальная информация предприятия, если информация уязвима, есть шанс ее неправомерного использования.

В наши дни современные и развитые с точки зрения технологий страны, использующие Информационные технологии, очень серезно относятся к нарушениям безопасности в системах обработки и передачи информации. Наибольшие потери несут торговые и банковские сферы, обслуживаемые системами телекоммуникации. Если не уделить особое внимание системам защиты таких информационных систем, важные персональные данные могут попасть в руки злоумышленников и нанести ущерб, как локально, например в городе, так глобально, если под угрозой будет работа всей системы банка. Это может быть как безобидная шутка, так и существенные финансовые потери, вплоть до банкротства компании.

Так как обмен информацией в ИТ осуществляется посредством компьютерных сетей, то необхдимо обеспечить должный уровень защиты в этих сетях. Нарушение безопасности в этом случае можно классифицировать как компьютерное преступление. В Европе существует организация, специализирующаяся на таких преступлениях «Europol», а в США «Federal Bureau of Investigation Internet Crime Complaint Center(IC3)».

Бывают пассивные и активные угрозы в сети. Пассивными называют угрозы, не влияющие на информационный процесс, например, анализ трафика и прослушивание. Активными называют угрозы, изменяющие или нарущающие работы информационного процесса, такие как: модификация данных, подделка данных, программые закладки и вирусы, блокирование работы компонентов ИС.

1.2 Исследование PWC SURVEY.

Согласно исследованию, проведенному PWC в рамках «Key findings from the Global State of Information Security® Survey 2017», многие собственники бизнеса и предприниматели, осознают, что именно они несут

ответственность за кибербезопасность и угрозы приватности. Но они не понимают, как разработать, внедрить и обслуживать системы защиты от угроз в реальном времени.

—52% имеют средства обнаружения вторжений

—51% Мониторинг и анализ информации

—48% Провели оценки уязвимости

—47% Провели оценки угроз

—47% Имеют средства защиты информации и средства управления событиями

—44% Проводили тесты на защищенность

PwC, CIO and CSO, The Global State of Information Security® Survey 2017, October 5, 2016

Управление угрозами требует комплексного подхода, и должна быть последовательной и точной, как партия в шахматы, в стратегическом и аналитическом мышлении. Рассмотрим четыре ключевых фактора, определяющих эффективность информационной безопастности:

1. Мониторинг и отслеживание входных и выходных параметров ИС.
2. Оценка воздействия входных и выходных параметров на ИС.
3. Идентификационные действия по «смягчению» угроз.
4. Немедленное принятие мер по устранению угрозы.

2. Теоретические сведения

2.1 Оценивание рисков безопасности информационной системы.

Использование информационных систем и технологий сопряжено с использованием различных средств и процессов, которые, в свою очередь, могут иметь уязвимости. Оценка рисков в области информационной безопасности позволяет контролировать эффективность защиты и целесообразность принятых мер.

В основе рисков нарушения конфиденциальности и целостности информации лежат уязвимости и угрозы разного характера, как

существующие, так и потенциальные. Важно приводить безопасность в актуальное состояние согласно классификации угроз. Контроль должен быть непрерывным, в то время как переоценка рисков может быть периодической.

Первоначальная оценка, при правильном выполнении, оказывает важное влияние и упрощает дальнейшее функционирование информационной системы. На протяжении жизненного цикла системы управление рисками может иметь максимальный эффект при минимальных затратах. Основные этапы жизненного цикла ИС:

—Инициализация, подготовка к работе

—Установка, настройка

—Эксплуатация

—Выведение из эксплуатации

—Прежде всего, перед процессом определения оценки, необходимо задать рамки для рассматриваемой информационной системы, ресурсов, которые она использует и обрабатываемой информации.

—архитектура ИС;

—применяемое аппаратное обеспечение;

—применяемое программное обеспечение;

—системные интерфейсы (внутренняя и внешняя связность);

—топология сети;данные и информация, область их применения;

—персонал и пользователи;

—процессы, выполняемые ИС;

—критичность системы и данных;

—требуемый уровень защищенности системы и данных.

2.2 Угрозы, средства предотвращения.

Процесс перехода потенциальной угрозы в реальную определяется жизненным циклом угрозы, который представлен процессом:

1. Зарождение, или появление признаков, косвенно или напрямую связанных с возникающей угрозой

2. Развитие, или увеличение числа таких признаков, превышение порогов, определяющих функционирование системы в нормальных условиях

3.1 Реализация, или внесение нестабильности в информационный процесс, нарушение его работы.

3.2 Нейтрализация, или устранение угрозы.

Развивающийся бизнес ставит перед собой все новые цели, достигать которые помогает сфера информационных технологий. В последние годы ИТ структуры развиваются в быстром темпе и становятся более динамичными. Обеспечивая должный уровень безопасности, профессионалы в области информационной безопасности усовершенствуют, согласно требованиям времени. системы управления безопасностью, такие как файерволы, системы обнаружения вторжений, и списки контроля доступа. Несмотря на успехи в этой области, атаки в киберпространстве продолжаются, так как появляются все новые способы обхода защиты, что в свою очередь влечет, например, кражу интеллектуальной собственности и ценных данных.

Почему так происходит? Пока системы безопасности эффективно выполняют свою работу, они также генерируют большие объемы информации. Лог-файлы, файлы кофигураций, отчеты-все это создает слишком большой массив данных, которые сложно обработать оперативно в ручном режиме, что затрудняет построение целостной картины и не дает готовые инструкции к действию. Без комплексного подхода к мониторингу, анализу и управлению, достичь приемлемого результата будет очень сложно.

Что нужно сделать, чтобы повысить защиту сетевой инфраструктуры и закрыть пробелы в безопасности?

—Составить топологию сети

—Защитить критичные данные с помощью проактивного анализа

—Планово проводить соответствие требованиям защиты

—Найти и задать высокий приоритет самым большим рискам

—Эффективно отвечать на атаки, согласно приоритету

—Внедрить постоянный процесс, чтобы убедиться, что все правила доступа заданы в соответствии с планом.

2.3 Регулирующие документы

Вопрос в настоящее время стоит очень остро, чем руководствоваться при создании модели угроз, есть ли готовые шаблоны. Для ответа на этот вопрос обратимся к ГОСТ Р 52448-2005, который гласит:

—Характеристика ресурсов коммуникационной структуры (объектов безопасности) сети связи, которые требуют защиты

—Рассмотрение возможных мест появления воздействий, носящих характер дестабилизации

—Этапы времени жизни сети

—Описание путей возникновения угроз и возможностей их реализации на практике

—Также важно добавить следующие элементы:

—Список всех возможных угроз

— Журнал всех зафиксированных нарушений безопасности, и подробное описание условий, вызванных нарушением

Можно также обратиться к ГОСТ Р 51344-99:

—Характеристика оборудования (техусловия, область применения, использование по назначению)

—Любые относящиеся к делу предположения, которые были сделаны (например, факторы безопасности и т.д.)

—Идентифицированные опасности

—Информация, на основании которой сделана оценка и определение риска (использованные данные и источники)

—Сомнения, связанные с использованными данными и источниками

—Цели, которые должны быть достигнуты защитными мерами (например, конфиденциальность, целостность и т.д.)

—Меры безопасности, принимаемые для устранения выявленных опасностей или уменьшения риска

—Остаточные риски.

Рассмотрим, в дополнение к двум предыдущим, ГОСТ Р 51901.1-2002, согласно которому модель угроз должна строиться по следующему сценарию:

—Краткое изложение анализа

—Выводы

—Цели и область применения анализа

—Ограничения, допущения и обоснование предположений

—Описание соответствующих частей системы

—Методология анализа

—Результаты идентификации опасностей

—Используемые модели, в т.ч. допущения и их обоснования

—Используемые данные и их источники

—Результаты оценки величины риска

—Анализ чувствительности и неопределенности

—Рассмотрение и обсуждение результатов

—Рассмотрение и обсуждение трудностей моделирования

—Ссылки и рекомендации.

Следуя указаниям ГОСТов можно составить модель угроз, однако такая модель будет статичным описанием гипотетических угроз. У нас будет вполне конкретный набор таких угроз, который будет представлять высокоуровневую структуру без конкретных указаний к применению на

практике. Другими словами схема, описывающая взаимосвязь компонентов и их свойства.

Возьмем, например, уязвимости в канале между узлами. Отчетливо сказать, где и на каких узлах уязвимость сложно, если в сети более 50 рабочих машин и установлена система обнаружения вторжений.

Нельзя защитить то, что не видно. Отталкиваясь от этого утверждения, чтобы создать динамическую модель защиты от угроз, у нас должна быть динамическая модель угроз, или достоверная система прогнозирования. Она создается единожды, а затем меняется по мере необходимости, или при изменении инфраструктуры сети, закрывая таким образом новые уязвимости, которые непосредственно влияют на появление возможных низкоуровневых угроз. В данном случае мы работаем с набором характеристик, значения которых изменяется в процессе работы системы. Таким образом мы имеем возможность адаптировать защитные механизмы к новым угрозам.

Принимая во внимание жизненный цикл угрозы, система обеспечения безопасности должна соответственно работать на всем промежутке жизненного цикла атаки. На первоначальном этапе производится обнаружение и устранение уязвимостей при помощи систем анализа защищенности. На следующем этапе-воплощения атаки в жизнь и ее завершения, данным действиям противостоят СОВ(системы обнаружения вторжений). Актуальные способы построения сетей имеют в свей основе достаточно сложную архитектуру и состоят из большого числа различных взаимосвязанных модулей или компонентов, выполняющих определенные функции. Для защиты локальных вычислительных сетей может использоваться многоагентная система, анализ выходных данных которой поможет выявлять вторжения с помощью выявления отклонений текущей активности от эталонной. Система должна обладать свойствами

масштабирования и адаптации, чтобы подстраиваться под появляющиеся уязвимости и новые методы злоумышленников.

В информационной безопасности имеется разрыв между двумя подмножествами. В первом из них находятся угрозы и риски, которые являются базой для создания моделей неблагоприятных ситуаций, оценки потерь и принятия мер по противодействию. Во втором располагаются уязвимости, атаки и признаки атак, позволяющие проанализировать систему на предмет наличия уязвимостей или определить фазу атаки. Встает проблема о том, что системный анализ и реализация в техническом плане не связаны. Отсутствие прямой связи между угрозами и уязвимостями.

2.4 Субъектно-объектная модель

Систему можно описать Субъектно-объектной моделью, рассматривая с позиции информационной безопасности.

Разобьем систему на два множества: объекты и субъекты. Объекты являются пассивным компонентом и хранят информацию, соответственно для них должна быть обеспечена конфиденциальность, целостность и доступность(файл, диск). Субъекты, в сою очередь, компоненты активные(DHCP, DNS, другие службы), которые выполняются на ЭВМ. Субъекты взаимодействуют с объектами посредством определенного множества операций, выполняемыми над объектами. Субъекты реализуют потоки непосредственно связанные с объектами и являются базовой метрикой(элементарные потоки работы с объектами: write, read, create, delete).

Получается, формальным образом субъектно-объектная модель представляется:

<A,B,C>, где

A — входящие в множество объекты $A=[a_i]$, $i=1,2 \dots n$;

B — входящие в множество субъекты $B=[B_j]$, $j=1,2 \dots m$;

C — множество операций в системе(объект-субъект) $C=[c_k]$, $k=1,2 \dots l$;

2.5 Построение карты сети

В настоящее время существует проблема реализации на практике подобной модели: для создания гарантированной защищенности требуется внешнее средство контроля неизменности конфигурации субъектов.

Важное место в построении системы анализа рисков сетевой безопасности занимает построение актуальной карты сети. Сделать это можно путем сбора конфигураций устройств в сети третьего уровня(маршрутизаторы, балансировщики нагрузки) и средства защиты информации(межсетевые экраны, системы предотвращения атак). На основе полученных данных от подключения к устройствам, либо из заданного хранилища(файловые ресурсы, база данных управления конфигурации) в автоматическом режиме строится актуальная карта сети(рис. 1).

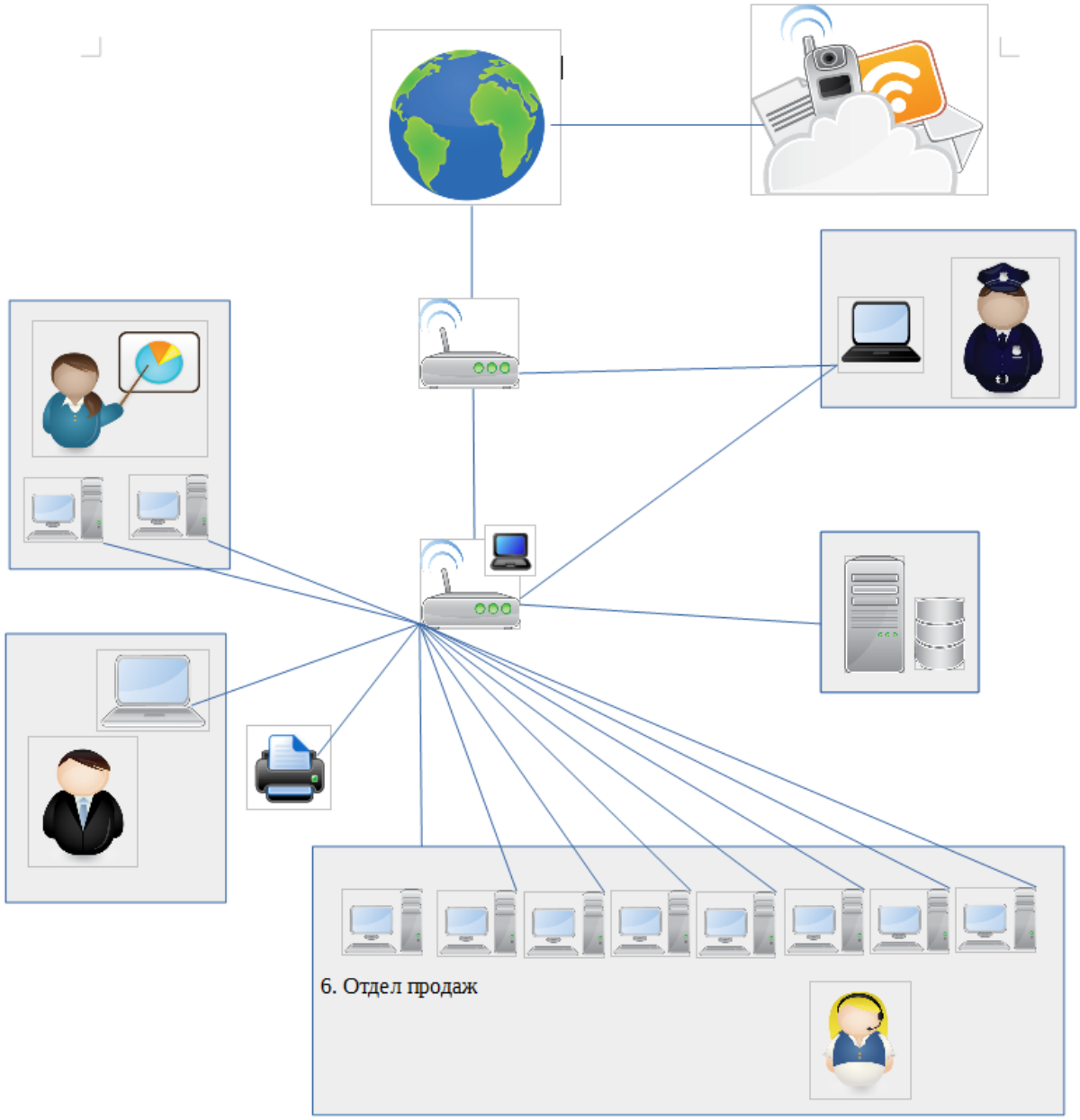

Рисунок. 1 Карта сети

Для удобства отображения, сетевые устройства, средства защиты информации и сегменты сети можно разделять по группам(офисы, филиалы), чтобы в будущем наглядно проанализировать политики и контроль доступа.

На следующем этапе необходимо провести проверки на предмет наличия уязвимостей в системе, определить возможные неправильные настройки при вводе в эксплуатацию. Также нужно удостовериться, что

данные настройки соответствуют стандартам по информационной безопасности, например, можно взять из открытого источника NVD Complete Vulnerability Listing(https://nvd.nist.gov/full_listing.cfm). Проверка эффективности примененных настроек с помощью стресс теста позволит выявить избыточные или неиспользуемые правила.

Основываясь на этой модели, можно проверить доступность узлов и корректность разграничения доступа между сегментами сети. В данном случае мы можем выявить потенциальные нарушения политик сетевого доступа.

Очередным важным шагом будет проверка доступности из внешней сети внутренних ресурсов локальной сети. Для этого необходимо построить все возможные маршруты с точностью до всех устройств, которые принимают участие в обмене пакетами данных, учитывая правила файервола, фильтрующих данные пакеты.

На основе вышеизложенных данных строится карта возможных векторов атак угроз и вторжений. Необходимо учитывать как прямые, так и косвенные атаки.

Данная информация помогает определить, каким участкам или сегментам сети необходимо уделить наибольшее внимание. Внося изменения в настройки безопасности, можно в реальном времени отслеживать изменения на модели сети, какие, например, появились угрозы, исходя из уязвимостей, и какие уязвимости были устранены.

В процессе построения модели сети важно учитывать приоритетные уязвимости, устранение которых защитит от атак приносящих наибольший ущерб.

После завершения всех настроек переходим к мониторингу-постоянной проверке всех несанкционированных изменений политик и настроек в сети. При обнаружении такого рода изменений, система может

передавать информацию о случившемся ответственному за ИБ администратору сети.

Оценка вероятного ущерба.

Стандарт Common Vulnerability Scoring System(общая система оценки уязвимостей) был разработан инженерами по безопасности NIAC. Свой вклад привнесли эксперты из Cisco, eBay, IBM Internet Security Systems, Microsoft, Symantec и др.

CVSS предлагает из себя открытую схему для расчета числового показателя по десятибалльной шкале, которая в явном виде отражает возможность потенциального ущерба-чем выше значение, тем более серьезная уязвимость имеет место быть и тем более оперативное вмешательство по ее устранению необходимо.
В стандарт включены три базовые метрики(оценок):

—Базовые метрики. Описание характера уязвимости.(параметры доступа, аутентификации, целостности, доступности и конфиденциальности.)

—Временные метрики отражают изменяющиеся во времени характеристики.

—Контекстные метрики -характеристики, уникальные для конкретного случая.

Временные и контекстные метрики дополнительные и используются для расчета оценки опасности с высокой точностью, характерной для рассмотренной уязвимости. Из этого следует, что потенциальный ущерб может быть рассчитан как влияющие на важную информацию уязвимости и возможный ущерб от появления рисков на основе данных уязвимостей.

$C_{Vj} = P \times CVSSScore$

C_{Vj} -вероятный ущерб

P -стоимость ресурса

$CVSSScore$ -коэффициент.

3.Динамическая модель управления безопасностью в локальной вычислительной сети

Этапы построения динамической модели модели информационной безопасности.

Рассмотрим синтез модели решения для управления информационной безопасностью информационной системы, в нашем случае для локальной вичислительной сети.

Основное место в обеспечении безопасности занимает человек, и принимаемые им решения на основе модели. Под термином объект в дальнейшем будем понимать соответствующее объекту описание или представление, которое дает достаточное соответствие объекту и характеризует этот объект в некоей мере. Исходя из этого следует, что решение есть модель процесса, с которой непосредственно работает человек.

Процесс это объект в состоянии функционирования при фиксированном предназначении.

Для синтеза применяем естественно-научный подход, базирующийся на законе целостности объекта.

В основе закона сохранения целостности объекта лежит тесная и постоянная взаимосвязь свойств объекта и свойств действия, при этом сохраняется изначальное предназначение объекта и процесса.

Представим процесс тремя компонентами, в соответствии с естественно-научным подходом(Рис. 2):

—Объективность(объект)

—Целостность(предназначение)

—Изменчивость(действие)

Рисунок 2. Декомпозиция управленческого решения

Интерпретируем эти компоненты в различных уровнях познания мира

1. абстрактном(методологический уровень)
2. абстрактно-конкретном(методический уровень)
3. конкретном(технологический уровень)

На рисунке представлена структурная схема развертывания содержания понятия «Решение».

Введём следующие определения:

Управленческое решение – управляемое состояние среды, обеспеченное субъектом для реализации предназначения объекта, в соответствующей обстановке в интересах достижения цели управления.

Обстановка – совокупность факторов и условий, в которых осуществляется деятельность.

Информационно-аналитическая работа – непрерывное добывание, сбор, изучение, отображение и анализ данных об обстановке. Например, разведка и мониторинг.

Чтобы реализовать синтез модели решения, нужно разложить управленческое решение на обстановку, мониторинг, и само решение.

На Рисунке 3 представлена структурная схема синтеза модели.

Модель может быть построена как на основе анализа, так и на основе синтеза, как известно из системотехники. Однако, подход, базирующийся на анализе имеет ряд недостатков, самым существенным из которых является невозможность формирования процесса с заранее известными свойствами, что является очень важным параметром в обеспечении безопасности информационного процесса.

Базирующийся на синтезе метод лишен недостатка из подхода на основе анализа, а также явно показывает достижение цели. Таким образом, исходя из вышеизложенных замечаний, целесообразнее применять в работе синтез модели управления информационной безопасности.

3.1 Синтез динамической модели управления решениями

Синтезируем модель, применяя свойства целостности и познаваемости.

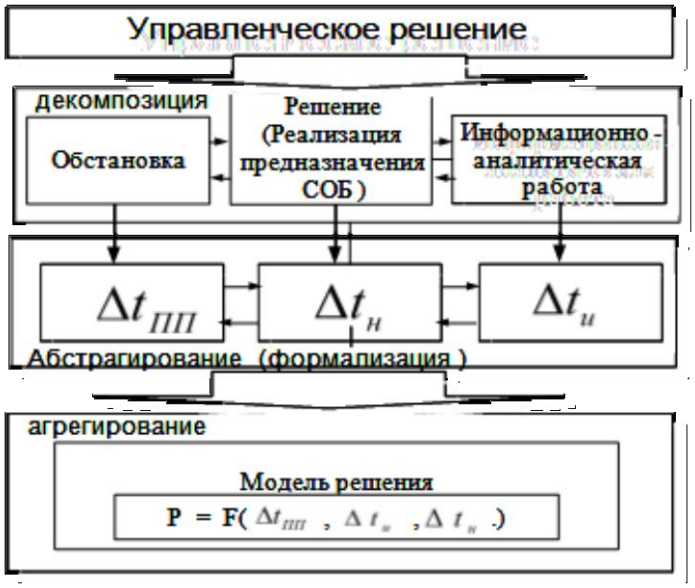

Рисунок 3 – Структурная схема развёртывания содержания процесса синтеза математической модели решения.

3.2 Условие существования процесса управления

Применив метод декомпозиции, на первом этапе, разобьем решение на три ранее определенных компонента:

Обстановка(объект)

Решение(предназначение)

Информационно-аналитическая работа(действие)

Далее, на втором этапе, с помощью метода абстрагирование, соотносим следующие элементы:

Элемент системы	Отождествляемый элемент
Объект(обстановка)	$\Delta t_{\text{пп}}$ периодичность проявления проблемы
Предназначение(решение)	$\Delta t_{\text{нп}}$ Периодичность нейтрализации проблемы
Действие(Информационно-аналитическая работа)	$\Delta t_{\text{ип}}$ Периодичность идентификации проблемы

—$\Delta t_{\text{ип}}$ Среднее время адекватным реагированием на проблему$_{\text{С}}$

—$\Delta t_{\text{нп}}$ Среднее время адекватным реагирования на проблему

—$\Delta t_{\text{ип}}$ Среднее время распознавания ситуации

Время-ценнейший невосполнимый ресурс человека, использование временных характеристик позволяет наглядно, на основе диаграммы изменения базовых компонентов формировать представление о модель решения.

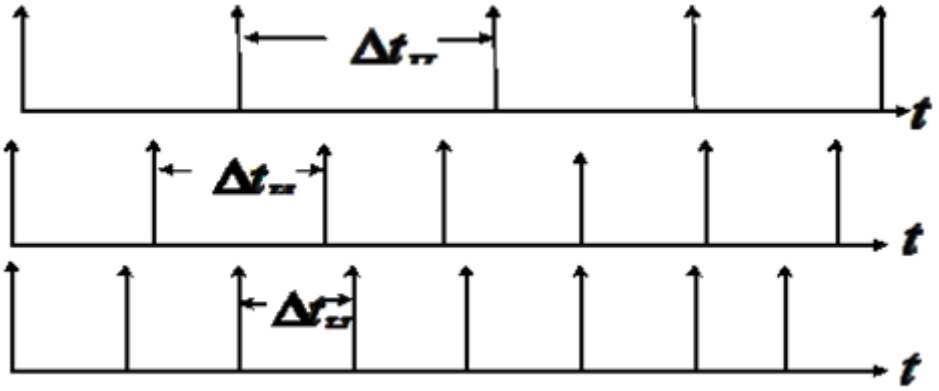

Рисунок 4 – Диаграмма проявления базовых элементов формирования модели решения.

3.3 Синтез модели управления безопасностью вычислительной локальной сети.

Исходя из данных, полученных в результате применения методов абстрагирования и агрегирования, преобразуем понятие управленческого решения в математическую модель управленческого решения вида:

$$P=F(\Delta t_{ПП},\ \Delta t_{ИП},\ \Delta t_{НП})$$

В этом и есть условие существования процесса управления информационной безопасностью информационного процесса. Так как управленческое решение состоит из трех элементов, представим структурную схему в виде

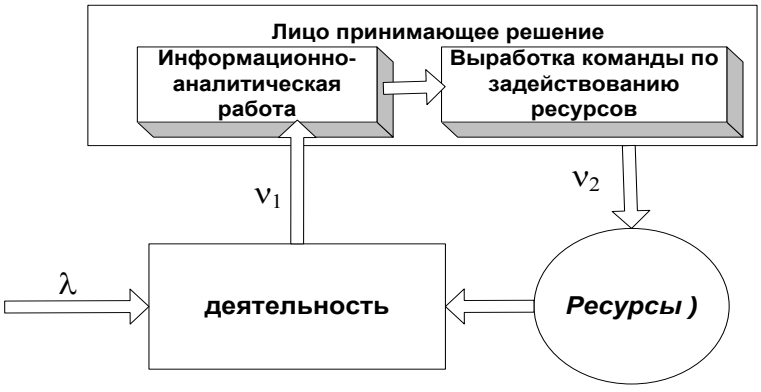

Рисунок 5 -Структурная схема управления деятельностью по обеспечению ИБ

На рисунке 5 обозначены:

 – величина, обратная среднему времени проявления проблемы;

ν_1 – величина, обратная среднему времени идентификации проблемы;

ν_2 – величина, обратная среднему времени нейтрализации проблемы.

Лицо принимающее решение при управлении информационной безопасностью может выполнять в различных сочетаниях две функции:

—идентифицировать (распознавать) проблему;

—нейтрализовать (задействовать ресурсы обеспечения ИБ) проблему.

Выделим 4 базовых состояния:

A_{00} – ЛПР не идентифицирует и не нейтрализует;

A_{10} – ЛПР идентифицирует и не нейтрализует;

A_{01} – ЛПР не идентифицирует и нейтрализует;

A_{11} – ЛПР идентифицирует и нейтрализует.

Для каждого из четырех состояний найдем вероятности, в которых может находится система управления безопасности, это соответственно P_{00}, P_{10}, P_{01}, P_{11}. Для формирования решения воспользуемся непрерывной цепью Маркова, так как мы имеем случайный процесс с дискретными состояниями и непрерывным временем, а также переход системы из состояния в состояние происходит в случайные моменты времени, а не в фиксированные. При рассмотрении таких процессов принято представлять переходы системы из одного состояния в другое под влиянием некоторых потоков событий.

Для реализации такого подхода составим систему дифференциальных уравнений Колмогорова-Чепмена. Примем, что первоначально система находится в состоянии A_{00}. После появления проблемы под воздействием интенсивности система переходит в состояние распознания проблемы A_{10}. Далее под воздействием интенсивности ν_1 происходит переход в состояние A_{01} в котором происходит процесс нейтрализации проблемы с интенсивностью ν_2 и

далее перевод системы в состояние $A_{00.}$ Такой исход возможен в случае, если одна проблема распознана, а другая проблема еще не образовалась. И далее процесс повторяется.

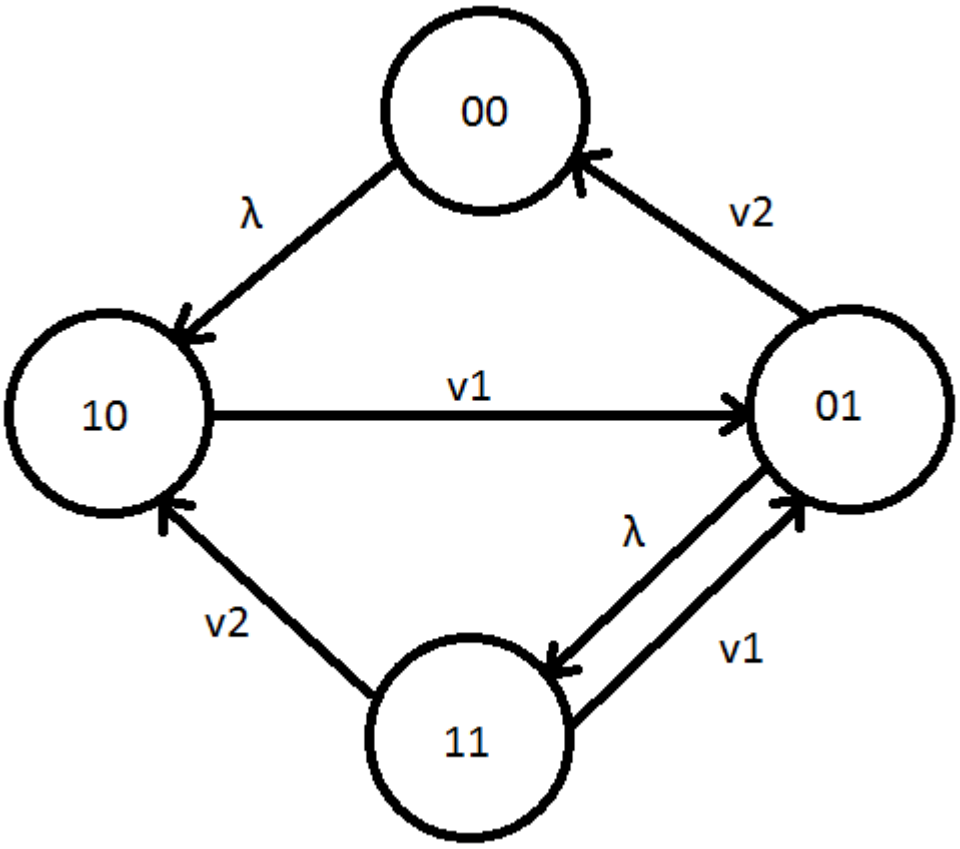

Рисунок 6. Граф состояний, процесса формирования управленческого решения

Для описания процесса изменения состояний на графе необходимо сделать следующие допущения и предположения.

1.Рассматривается схема формирования решения человека в форме информационно-управляющей системы. На основе решения формируется процесс обеспечения ИБ.

2. Промежутки времени между моментами обнаружения фактов проявления проблем являются величинами случайными.

3. Обнаруженные факты во времени образуют поток, близкий к потоку Пуассона.

4. Время обработки данных о требуемом признаке является величиной случайной.

5. Данные о признаках распределяются далее между выделенными ресурсами, решающими соответствующие целевые задачи по обеспечению ИБ.

6. Рассматривается случай, когда время пребывания требуемых признаков (фактов) в области действия системы (человека) весьма ограниченно и соизмеримо со временем, которое необходимо для их идентификации, а также обработки данных и принятия адекватных действий по этим признакам.

7. Система подготовлена к решению задач распознанию и нейтрализации проблем.

8. Разрабатываемая система (решение человека) предназначена для оценивания потенциальных возможностей системы обеспечения ИБ в зависимости от обстановки.

Введённые допущения и предположения позволяют использовать систему дифференциальных уравнений Колмогорова - Чепмена. Тогда составим систему ДУ Колмогорова для нашей ситуации. Она будет иметь следующий вид:

$$\begin{aligned}
&\frac{d}{dt}P_{00}(t) = -P_{00}(t)\lambda + P_{01}(t)\nu_2 \\
&\frac{d}{dt}P_{01}(t) = -P_{01}(t)(\lambda+\nu_2) + P_{11}(t)\nu_1 + P_{10}(t)\nu_1 \\
&\frac{d}{dt}P_{10}(t) = P_{00}(t)\lambda - P_{10}(t)\nu_1 + P_{11}(t)\nu_2 \\
&\frac{d}{dt}P_{11}(t) = P_{01}(t)\lambda - P_{11}(t)(\nu_1+\nu_2)
\end{aligned} \qquad (1)$$

Для системы ДУ (1) накладывается следующее ограничение:

$$P_{00}(t) + P_{10}(t) + P_{01}(t) + P_{11}(t) = 1. \qquad (2)$$

Система (1) решается для заданных начальных условий

1. В общем случае используем соотношения (3), где правые части некоторые константы – вероятности нахождения системы в соответствующих состояниях.

$$P_{00}(0) = P_{00*};\ P_{10}(0) = P_{10*};\ P_{01}(0) = P_{10*};\ P_{11}(0) = P_{11*} \qquad (3)$$

2. В случае, когда система находится в состоянии $A_{00,}$ то есть, проблема, на которую надо реагировать отсутствует, не рассматривается и не обрабатывается.

$$P_{00}(0) = 1;\ P_{10}(0) = 0;\ P_{01}(0) = 0;\ P_{11}(0) = 0; \qquad (4)$$

Рассмотрев процесс как динамический, перейдём к выявлению возможностей рассмотрения этого процесса как стационарного, не нарушая общности рассуждений. Такой подход позволит нам описывать этот процесс уже системой линейных алгебраических равнений. Если процесс, протекающий в системе, длится достаточно долго, то имеет смысл говорить о предельном поведении вероятностей $P_i(t)$ при $t \to \infty$. В некоторых случаях существуют финальные (предельные) вероятности состояний, где $i = 0, 1, \ldots, n$. $P_i = \lim_{t \to \infty} P_i(t)$

Они не зависят от того, в каком состоянии система S находилась в начальный момент. Говорят, что в системе S устанавливается предельный стационарный режим, в ходе которого она переходит из состояния в состояние, но вероятности состояний P_i уже не меняются.

Система, для которой существуют финальные вероятности, называется эргодической, а соответствующий случайный процесс – эргодическим. Финальные вероятности состояний, если они существуют, могут быть получены путем решения системы линейных алгебраических уравнений, которые получаются из дифференциальных уравнений Колмогорова, если приравнять производные к нулю, а вероятностные функции состояний $P_1(t)$,..., $P_n(t)$ в правых частях уравнений Колмогорова (2) заменить соответственно на неизвестные финальные вероятности P_1, … , P_n. Таким образом, для системы S c n состояниями получается си-

стема n линейных однородных алгебраических уравнений с n неизвестными P_0, P_1, …, P_n, которые можно найти с точностью до произвольного множителя. Для нахождения точного значения $P_0,P_1,\ldots,P_n$ к уравнениям добавляют нормировочное условие $P_0 + P_1 + ...+ P_n = 1$, пользуясь которым можно выразить любую из вероятностей P_i через другие и отбросить одно из уравнений.

Если предположить, что мы имеем стационарный процесс, тогда наша исходная система дифференциальных уравнений трансформируется в систему линейных однородных алгебраических уравнений следующего вида:

$$\begin{aligned}
&-P_{00}(t)\lambda+P_{01}(t)v_2=0;\\
&-P_{01}(t)(\lambda+v_2)+P_{11}(t)v_1+P_{10}(t)v_1=0;\\
&P_{00}(t)\lambda-P_{10}(t)v_1+P_{11}(t)v_2=0;\\
&P_{01}(t)\lambda-P_{11}(t)(v_1+v_2)=0.
\end{aligned} \qquad (5)$$

Это есть система линейных алгебраических уравнений относительно четырёх неизвестных P_{00} , P_{10}, P_{01}, P_{11}, которые связаны между собой следующим соотношением

$P_{00} + P_{10} + P_{01} + P_{11} = 1.$

Искомые вероятности уже не зависят от времени. Решением данной линейной алгебраической системы уравнений является следующие соотношения:

$$P_{00}=\frac{v_1v_2}{\lambda(\lambda+v_1+v_2)+v_1v_2} \qquad (6)$$

$$P_{10}=\frac{\lambda v_2(\lambda+v_1+v_2)}{(v_1+v_2)\left[\lambda(\lambda+v_1+v_2)+v_1v_2\right]} \qquad (7)$$

$$P_{01}=\frac{\lambda v_1}{\lambda(\lambda+v_1+v_2)+v_1v_2} \qquad (8)$$

$$P_{11}=\frac{\lambda v_1}{(v_1+v_2)\left[(\lambda+v_1+v_2)+v_1v_2\right]}$$

(9)

Получив соотношения, определяющие вероятности нахождения системы в состояниях A_{00}, A_{10}, A_{01}, A_{11}, мы можем выработать требования к свойствам процесса распознания проблемы, возникшей в системе и к свойствам процесса нейтрализации этой проблемы в системе обеспечения информационной безопасности.

$$P_{00} = P_{ОБСЛ} \frac{\nu_1 \nu_2}{\lambda(\lambda + \nu_1 + \nu_2) + \nu_1 \nu_2} \quad (10)$$

В этом соотношении связаны три параметра. Таким образом мы установили аналитическую зависимость обобщённых характеристик обстановки ($\Delta t_{пп}$), информационно-аналитической деятельности ($\Delta t_{ип}$) и нейтрализации проблемы ($\Delta t_{нп}$), возникшей при управлении безопасностью информационной системы.

Следуя работе академика Анохина П.К., мы получили системообразующий фактор создания системы управления процессом обеспечения ИБ в форме соотношения (10).

3.4 Технология управления процессом обеспечения ИБ

3.4.1 Общий подход к разработке технологии управления процессом обеспечения ИБ

Общий подход к разработке технологии управления процессом обеспечения ИБ проходит в несколько этапов.

1 этап. Обоснование оценивания.

Обоснование требует:

1) Установить уровень опасности в системе в зависимости от воздействующих на нее угроз

2) Разработать методику обоснования путей снижения уровня информационной опасности до допустимого уровня

Оценивание позволяет:

1) Обосновать рациональные действия и способы их реализации на основе разработанной модели

2) Обосновать возможности системы обеспечения безопасности

3) Предъявить требования к возможностям лица принимающего решения

2 этап. Формирование показателя эффективности реализации управленческого решения.

$P_{ИНП}=F(\Delta t_{ср/ПП},\ \Delta t_{ср/ИП},\ \Delta t_{ср/НП})$

Так же, на 2 этапе вероятность того, что каждая угроза будет идентифицирована (система мониторинга) и нейтрализована (Силы и средства силы и средства обеспечения безопаности) определяется соотношением:

$$P_{ИНП} = P_{00} = \frac{\nu_1 \nu_2}{\lambda(\lambda + \nu_1 + \nu_2) + \nu_1 \nu_2}$$

Компоненты этого соотношения определяются на основе решения системы дифференциальных или алгебраических уравнений в зависимости от допущений и предположений.

3 этап. На основе зависимости трёх базовых компонентов управленческого решения и заданного уровня показателя эффективности Р строятся система параметрических поверхностей, образованных концом вектора Р трёх координатной системе:

– «Обстановка» - $\Delta t_{\lambda}=f_{\lambda}(x_1,x_2,\ldots,x_n)$

– «Информационно–аналитическая работа» $\Delta t_{v_1}=f_{v_1}(y_1,y_2,\ldots,y_m)$

– «Обеспечение субъектом реализации предназначения СОБ в соответствующей обстановке» - $\Delta t_{v_2}=f_{v_2}(z_1,z_2,\ldots,z_k)$

4 этап. На основе параметрических представлений управленческого решения, сформированных на третье этапе вырабатываются требования к

мониторингу, системе обеспечения безопасности и возможностям ЛПР. (В настоящей работе не рассматривается)

5 этап. Средой в информационном канале сети, в котором размещёна Информационная система, генерируются угрозы различного характера и направленности с периодичностью $\Delta t_{ПФ}$. На λ наложены ограничения вида:

$$\int_T \lambda(t)\,dt = W$$

6 этап. Поток информационных угроз, характеризующий спрос на деятельность СОБ «обслуживается» информационно-управляющей системой. Информационный компонент осуществляет мониторинг и выявляет с интенсивностью ν_1 потенциальные потребности в задействование СОБ. При ограничениях на информационный ресурс:

$$\int_T v_1(t)\,dt = V_1,$$

7 этап. По результатам мониторинга ЛПР с периодичность Δt (с интенсивностью ν_2) вырабатывает решение по нейтрализации угроз, которое гарантированно отрабатывает СОБ. При ограничении на деятельностный ресурс:

$$\int_T v_2(t)\,dt = V_2$$

3.5 О возможностях сетевого моделирования

Сетевое моделирование позволяет решать отдельные задачи при задании небольшого количества сочетаний исследуемых параметров системы.

Основными параметрами сетевого графика являются:

1) Наиболее раннее возможное время наступления j-го события Tp (j), вычисляемое по формуле:

$$T_P(j) = \max_{i \subset j} (T_P(i) - t_{ij}) \qquad \textbf{(3.1.)}$$

где символами

- **i и j** обозначаются номера предшествующего и последующего событий соответственно;

-$\mathbf{t_{ij}}$ — продолжительность **(i, j)** -й работы.

Из обозначения $i \subset j$ следует, что событие i предшествует событию j.

2) Самое позднее допустимое время наступления i-го события $T_п$ (i), вычисляемое по формуле

$$T_П(j)=\frac{\min}{i \supset j}(T_П(i)-t_{ij}) \qquad \textbf{(3.2)}$$

где из обозначения $i \supset j$ следует, что событие j предшествует событию i

3) Резерв времени данного события R_i, вычисляемый по формуле

$$R_i=(T_П(i)-T_P(i)) \qquad \textbf{(3.3.)}$$

4) Полный резерв времени работы $r_п$ (i,j), вычисляемый по формуле

$$r_П(\mathrm{i,j})=(T_П(j)-T_P(i)-t_{ij}) \qquad \textbf{(3.4.)}$$

Смысл полного резерва времени работы заключается в том, что задержка в выполнении работы (i,j) на величину $\Delta \mathbf{t_{ij} \geq r_п (i,j)}$, приводит к задержке в наступлении завершающего события на величину (Δt_{ij} - $r_п$ (i,j)).

5) Свободный резерв времени работы r_c (i,j), вычисляемый по формуле

$$r_c(\mathrm{i,j})=(T_P(j)-T_П(i)-t_{ij}) \qquad \textbf{(3.5.)}$$

Смысл свободного резерва времени работы заключается в том, что задержка в выполнении работы на величину $\Delta \mathbf{t_{ij} \leq r_C(i,j)}$, не влияет ни на один другой срок, определенный данным сетевым графиком.

Основными показателями сетевого графика, по которым выполняется его анализ, являются:

1) Критический путь — это полный путь, на котором суммарная продолжительность работ является максимальной. Иными словами, это самый длинный по времени путь в сетевом графике от исходного до завершающего события. Критический путь лимитирует выполнение

операции, поэтому любая задержка на работах критического пути увеличивает время всего процесса. События, через которые проходит критический путь, и работы, лежащие на критических путях, называются напряженными. У критических работ как полные, так и свободные резервы времени равны нулю (признак критической работы). Критический путь рассчитывается путем определения работ, полные резервы времени которых равны нулю.

2) Полный резерв времени ненапряженного пути — это резерв времени ненапряженных событий и работ, т. е. тех, которые лежат не на критическом пути. В том случае, если ненапряженный и критический пути не пересекаются, полный резерв времени ненапряженного пути равен разности между его длиной и длиной критического пути (во временной мере). Если ненапряженный и критический пути пересекаются, полный резерв времени равен самому длительному участку ненапряженного пути, заключенному между соответствующими парами событий критического пути. Полный резерв времени ненапряженного пути показывает, на сколько в сумме может быть увеличена продолжительность всех работ этого пути без изменения срока выполнения операции в целом.

Сущность анализа сетевого графика заключается в том, что выявляются резервы времени работ, лежащих на ненапряженных путях, и направляются на работы, лежащие на критическом пути, который лимитирует срок завершения работы в целом. Этим достигается сокращение времени выполнения критических работ, а значит, и всей операции.

3) Время выполнения работ (временные оценки работ) может определяться либо по нормативам (статистическим показателям), либо при отсутствии их — по следующим эмпирическим формулам:

$$\bar{t}_{ij} = \frac{t_{\min} + 4t_{H.B} + t_{max}}{6} \qquad \textbf{(3.6.)}$$

$$\sigma_{ij} = \frac{t_{\min} - t_{mix}}{6} \qquad \textbf{(3.7)}$$

где $\bar{t}_{ij}$ — математическое ожидание продолжительности выполнения (i,j) работы (среднеожидаемое время работы) ;

σ_{ij} — среднеквадратическая ошибка в определении продолжительности работы;

t_{min} — продолжительность работы в наиболее благоприятных условиях (оптимистическая оценка);

t_{max} — продолжительность работы при самом неблагоприятном стечении обстоятельств (пессимистическая оценка);

$t_{H.B}$ — продолжительность работы при условии, что не возникает никаких неожиданных трудностей (наиболее вероятная оценка).

Математическое ожидание любого параметра сетевого графика, являющегося суммой величин t_{ij} равно $\sum \bar{t}_{ij}$

Среднеквадратическая ошибка в определении этого параметра равна $\sqrt{\sum \sigma_{ij}^2}$.

Вероятность свершения j –го события в расчётный срок $\mathbf{p_j}$ определяется по формуле $p_j = \Phi\left(\frac{T_З - T_P(j)}{\sqrt{\sum \sigma_{ij}^2}}\right)$

где Ф(…) — функция Лапласа;

$\mathbf{T_З}$ — заданный срок свершения события;

$\mathbf{T_P}$(j) — время раннего свершения j-го события;

σ_{ij} - среднеквадратические ошибки в определении продолжительности работ, которые использовались при вычислении раннего срока наступления j-го события.

3.6 Сетевые модели возникновения угроз, мониторинга и управления безопасностью.

3.6.1 Общая сетевая модель образования угрозы.

Появление угрозы зачастую может сопровождаться изменением параметров функционирования информационной системы. В общем виде сетевая модель может быть представлена в виде, изображенном на рисунке 7.

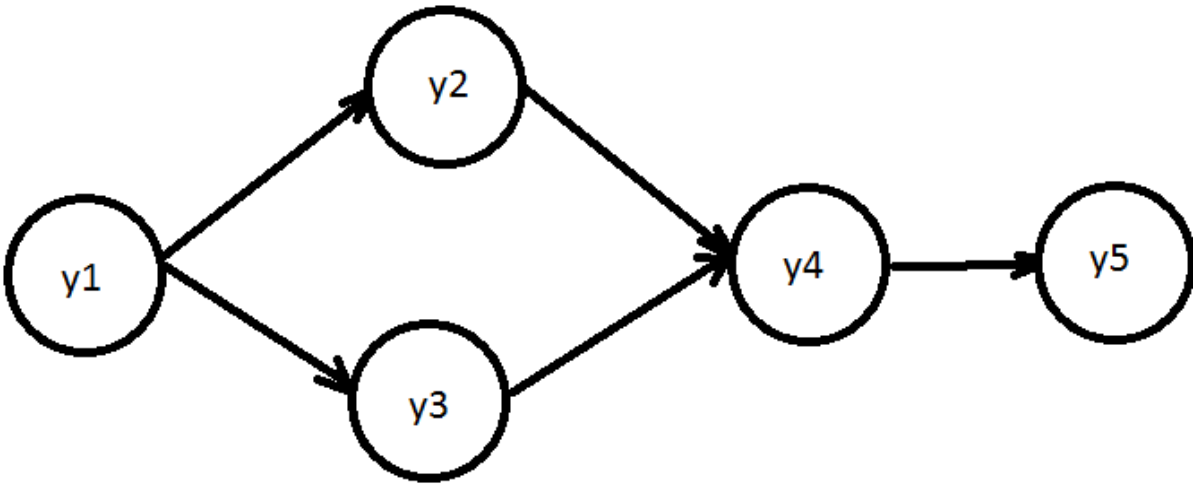

Рисунок 7. Сетевая модель угрозы.Общая сетевая модель угрозы локальной сети

Табл.1

Условное обозначение	Событие
y1	Появление угрозы
y2	Внутренняя
y3	Внешняя
y4	Мониторинг
y5	Нейтрализация.

3.6.2 Общая сетевая модель мониторинга угроз.

Для поддержания сети в работоспособном состоянии важен непрерывный контроль, так как в настоящее время любая сети используются в критически важных процессах от работы до расчетов.

Мониторинг - очень важный этап, без которого управление сетью представляется очень сложной задачей. Учитывая важность данной функции, ее можно отнести в отдельный модуль и реализовать специальными средствами. Применяя в работе автономные средства контроля помогает администратору ИБ выявлять проблемные участки и устройства сети, а при необходимости, отключать или производить перенастройку средствами управления в автоматическом режиме. В контроль входят этапы мониторинга и последующего анализа результатов.

На стадии мониторинга выполняется процедура сбора первичных данных о состоянии сети: проверка портов маршрутизаторов, коммутаторов, сбор и ведение журнала о количестве пакетов и кадров разных протоколов.

Следующим является стадия анализа, входящие в который процедуры обрабатывают полученную на стадии мониторинга информацию, сравнения с ранее полученными результатами и, на основании результатов, предоставление информации о вероятных причинах сбоев или ненадежной работе в сети

Подобные задачи решаются с помощью спектра устройств и программных средств, включающих в себя аппаратные и программные измерители, тестеры, сетевые анализаторы, агентами систем управления и др. В некоторых случаях для эффективного анализа может потребоваться использование знаний человека, или экспертных систем, в основе которых лежат знания и опыт специалистов в области информационной безопасности.

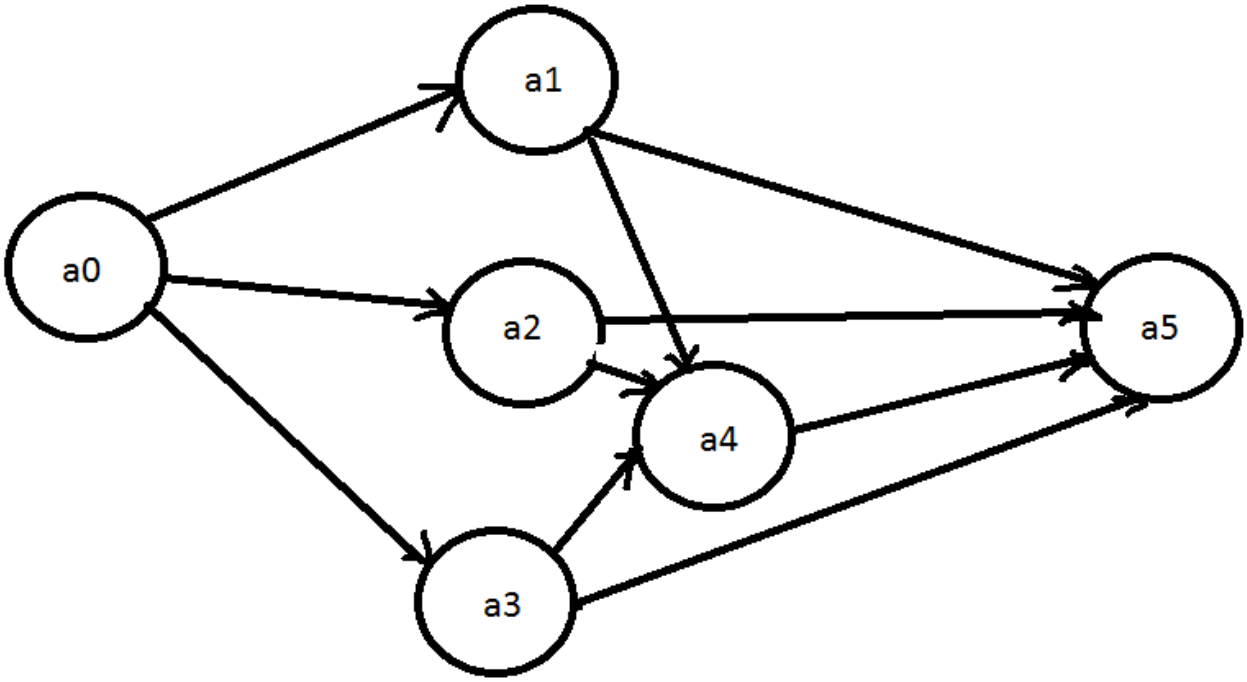

Рисунок 8. Сетевой график мониторинга

Общая сетевая модель мониторинга локальной сети

Табл.2

Условное обозначение	Событие
a0	Мониторинг сети
a1	Встроенные системы диагностики
a2	Анализаторы протоколов
a3	Сетевые анализаторы
a4	Экспертные системы
a5	Журнал тестирования

Анализ сетевого графика мониторинга сети

Основными параметрами сетевого графика являются:

1. Наиболее раннее возможное время наступления j-го события T_p (j), вычисляемое по формуле:

$$T_P(j)=\frac{\max}{i\subset j}(T_P(i)-t_{ij})$$, где

- i и j обозначаются номера предшествующего и последующего событий соответственно;

- t_{ij} — продолжительность (i, j) -й работы.

Из обозначения $i\subset j$ следует, что событие i предшествует событию j.

2. Самое позднее допустимое время наступления i-го события Тп (i), вычисляемое по формуле

$$T_П(j)=\frac{\min}{i\supset j}(T_П(i)-t_{ij})$$

где из обозначения $i\supset j$ следует, что событие j предшествует событию i

3. Резерв времени данного события Ri вычисляемый по формуле

$$R_i=(T_П(i)-T_P(i))$$

4. Полный резерв времени работы rп (i,j), вычисляемый по формуле

$$r_П(\text{i,j})=(T_П(j)-T_P(i)-t_{ij})$$

3.6.3 Общая сетевая модель управления безопасностью

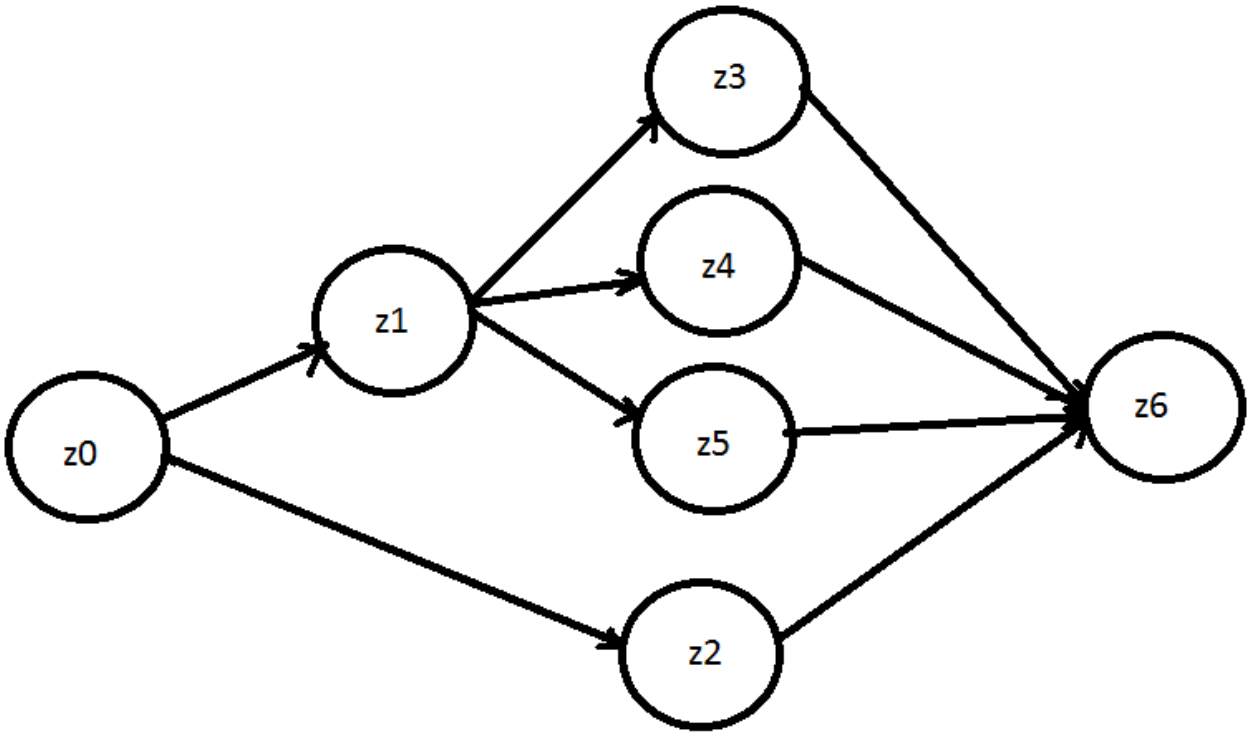

Рисунок 9. Сетевой график устранения проблемы

Табл.3

Условное обозначение	Событие
z0	Обнаружение проблемы
z1	Чтение журнала тестирования
z2	Применение исправления, исходя из выходных данных экспертной системы
z3	Применение исправления, исходя из выходных данных встроенных систем диагностики
z4	Применение исправления, исходя из выходных данных анализаторов протоколов
z5	Применение исправления, исходя из выходных данных сетевых анализаторов
z6	Проблема устранена

Основными параметрами сетевого графика являются:

1. Наиболее раннее возможное время наступления j-го события T_p (j), вычисляемое по формуле:

$$T_P(j)=\frac{\max}{i\subset j}(T_P(i)-t_{ij})$$, где

- i и j обозначаются номера предшествующего и последующего событий соответственно;

- t_{ij} — продолжительность (i, j) -й работы.

Из обозначения $i \subset j$ следует, что событие i предшествует событию j.

2. Самое позднее допустимое время наступления i-го события Тп (i), вычисляемое по формуле

$$T_П(j)=\frac{\min}{i \supset j}(T_П(i)-t_{ij})$$

где из обозначения $i \supset j$ следует, что событие j предшествует событию i

3. Резерв времени данного события Ri вычисляемый по формуле

$$R_i=(T_П(i)-T_P(i))$$

4. Полный резерв времени работы $r_п$ (i,j), вычисляемый по формуле

$$r_П(\mathrm{i,j})=(T_П(j)-T_P(i)-t_{ij})$$

3.7 Современные методы мониторинга

В настоящее время многие предприятия используют в своей работе сети и системы, различных масштабах: от объединения нескольких компьютеров, в небольшом офисе до глобальной сети - интернет. На данный момент требования к таким сетям очень высокие – они должны обеспечивать бесперебойную работу. Существует множество систем контроля безопасности имеющих в своей основе разные разработки и технологии, которые иногда могут оказаться несовместимы с другими подобными системами.

Однако последние разработки в области информационной безопасности изменили данный подход в сторону универсальности и унифицированности. Растущее число персональных компьютеров и соответственно растущее число автоматизированных рабочих мест увеличивает объёмы локальных вычислительных сетей (ЛВЛ), что неумолимо увеличивает сложность обслуживание данных сетей. Соответственно встаёт вопрос о том, как грамотно организовать и провести

диагностику и какие методы обеспечения информационной безопасности (ИБ) в вычислительных сетях можно использовать.

Под диагностикой следует понимать процесс постоянного не прерывающего анализа состояния вычислительной сети. Как только появляется дефект или неисправность сетевого устройства необходимо незамедлительно записать это событие в журнал, а так же по возможности локализовать и определить тип неисправности. Администратор информационной безопасности должен иметь доступ ко всей топологии сети, а так же к подробным техническим характеристикам всех устройств и интерфейсов. Более того, некоторым функциональным свойствам сети нужно уделить наибольшее внимание ещё на стадии её проектировки. В качестве системы для хранения таких данных подойдут специальные системы документирования сети. Используя эти данные, администратор ИБ будет иметь представление о скрытых уязвимостях своей системы, чтобы в момент чрезвычайного происшествия примерно знать, с чем связана данная проблема.

Рядовой пользователь не обращает внимания на работу сети, ему важно как работает прикладное программное обеспечение, возникающие коллизии, а так же ошибки передачи пакетов, степень загруженности канала и производительности сетевого оборудования - являются второстепенными для обычного пользователя.

3.7.1 Диагностика локальных сетей.

Большое количество компаний на рынке информационной безопасности предлагает свои услуги по защите вычислительных сетей, однако, не одна компания не может предложить стопроцентную защиту. Использование нескольких продуктов позволяет повысить защищенность сети.

На сегодняшний день стек протоколов IP стал самым распространённым в сети, что доказывает большое количество сайтов в

сети internet. Используемая сегодня технология волоконно-оптических кабелей позволила существенно снизить возможные неисправности в сравнении с прошлыми технологиями, например, медный или коаксиальный кабель. В аналоговых системах могут, появляется перекрёстные помехи, которые возникают в результате того, что излучение одного проводника порождает паразитное излучение на другом проводнике, а цифровые в свою очередь – лишены этого недостатка. Цифровой способ передачи информации по оптическим кабелям не поддаётся воздействию электромагнитными шумами и индуцированными сигналами, вследствие этого нет особенных требований к монтажу данных кабелей. Основным свойством данного типа передачи является сила сигнала или оптическая мощность. В случае если имеется возможность узнать как сигнал ослабевает(потери) на всей длине оптического канала, тогда благодаря этим данным представляется возможным идентификация почти любой проблемы.

Для анализа повреждений в линии можно воспользоваться оптическим временным рефлектометром. Данный прибор генерирует импульсные сигналы и анализирует их отражение, далее базируясь на данном анализе, он может показать есть ли в проводнике физические повреждения, либо другие отклонения, более того, прибор может приблизительно указать место возникновения проблем. Монтаж оптического волокна требует определённого уровня навыков, хоть многие производители стараются упрощать процесс монтажа. Следует принять во внимание тот факт, что всегда есть вероятность того, что кабель будет физически повреждён в результате непреднамеренных событий.

3.7.2 Инструменты, используемые для диагностики.

Одной из основных функций диагностики является непрерывное отображение состояние сети в данный момент времени. Инструменты

мониторинга в той или иной мере точно соответствуют уровням модели OSI.

Физический уровень.

Для мониторинга состояния на данном уровне используются кабельные тестеры, а так же специальные приспособления, например, рефлектометры. Рассмотрим данные приспособления подробнее:

—Разъём-заглушка.

Принцип работы данной заглушки, заключается в том, что выходная линия замыкается на входную, что приводит компьютер в состояния передачи данных самому себе. Используется в качестве инструмента для диагностики оборудования.

—Расширенный тестер кабеля.

Данное средство позволяет вести мониторинг трафика сети и отдельно взятого компьютера и на выходе давать данные о неисправности линии связи или сетевого оборудования.

—Рефлектометр.

Данное устройство используется в линии для определения неисправностей локационным (рефлектометрическим) методом.

Принцип работы: рефлектометр генерирует в кабеле короткие импульсы и позволяет находить разрывы, замыкание и прочие дефекты, так же выводит результаты протяженности кабеля и его волнового сопротивления.

—Тоновый генератор.

Это устройство генерирует импульсный или непрерывный тоновый сигнал, который проходя по каналу, даёт представление о целостности и качестве кабеля. Тоновый определитель на основе анализа тонового сигнала показывает параметры целостности и качества кабеля.

—Цифровой вольтметр.

Устройство позволяющее измерять напряжение тока и определять целостность сетевых кабелей.

Канальный, сетевой и транспортный уровень

Для обнаружения неисправностей на этих трёх уровнях используется анализатор протоколов. Подобные устройства собирают статистику о сетевых устройствах, сетевом оборудовании и о работе сети, так же они позволяют вести наблюдения и фиксировать изменения параметров объектов в сети.

Простые анализаторы протоколов могут быть созданы на основе любого портативного компьютера, который использует сетевую карту с поддержкой приёма всех пакетов. Однако, одним из существенных недостатков подобного анализатора является тот факт, что существует проблема мониторинга всех неполадок на канальном уровне. Следующим средством диагностики является зонд или монитор. Монитор сети – это программно- аппаратный комплекс, который следит за трафиком в сети и производит проверку пакетов на уровне кадров, также собирает данные о типах этих пакетов и ошибках в сети.

Мониторы сети, как правило, используются, и функционирую постоянно и непрерывно. Данные мониторы могут взаимодействовать с протоколами удалённого мониторинга RMON и RMON II. В протокол RMON входят функции сбора статистики информации о трафике и ошибках в сети. Протокол RMON использует в своей основе канальный уровень, в то время как в протоколе RMON II есть поддержка 3-го, 4-го, 5-го уровней. Более того протокол RMON II имеет возможность ведение журнала о собранных пакетах и кадрах.

Существующее средство программной реализации диагностики сети называется – системой управление сетью, и, по сути, представляет из себя систему, которая собирает данные о состоянии сети, оборудовании входящим в сеть и трафике. Подобные системы осуществляют не только

аналитическую работу, но и способны также в автоматическом или полуавтоматическом режиме воздействовать на объекты сети, например, управлять портами сетевых устройств или менять параметры и настройки коммутаторов и маршрутизаторов.

Средства управления системой.

Данная система близка по функционалу к системе управления сетью, но она может управлять коммуникационным оборудованием.

Экспертные системы.

Данные системы представляют из себя готовые шаблоны, полученные на основе работы с экспертами в области сетевых технологий. Примером экспертной системы может являться база знаний с модулем нейронных сетей, которая позволяет получать точный результат на основании данных мониторинга и анализа.

Средства диагностики и их техническое воплощение.

Диагностика кабельных систем.

Устройствами для диагностики кабельных систем являются:

—анализаторы

—тестеры

— кабельные сканеры

Сетевые анализаторы.

Принцип работы сетевого анализатора заключается в том, что по кабелю передаётся спектр сигналов, а на другом конце находится узкополосный приёмник. Полученные на узкополосном приёмнике, данные, позволяют нам, построить картину затухания. Подобные анализаторы являются дорогостоящим оборудованием и используются в лабораторных условиях.

Кабельные сканеры.

Такие устройства помогают определить длину кабеля и различные технические характеристики, а так же оценить выходные данные.

Принцип работы кабельного сканера, заключается в том, что устройство генерирует короткий электрический импульс в кабеле и далее определяет время возвращение отраженного сигнала. Полярность отраженного сигнала позволяет судить о наличии обрыва или замыкания кабеля. Если монтаж был произведён корректно, отраженный импульс будет отсутствовать. Точность данных приборов зависит от скорости распространения электромагнитных волн в канале и, как правило, является коэффициентом к скорости света в вакууме. Как правило, данные сканеры позволяют использовать для калибровки специальные таблицы данных, в которых содержится информация обо всех типах кабелей.

Тестеры кабельных систем.

Тестеры кабельных систем в сравнение с предыдущими являются менее дорогостоящим и более простыми устройствами. Функциональность тестеров кабельных систем заключается в том, что он может определить есть ли в кабеле разрыв, но в каком месте, точно не укажет.

В качестве дополнительных инструментов мониторинга могут выступать:

—Двустороннее тестирование

—проверка оптико-волоконных кабелей

—составление топологии сети

—составление подробной схемы соединения жил кабелями

—выявление импульсных помех

—мониторинг трафика в сети

—подбор программ для проведения тестов сети

—интегрированный генератор тональности для трассировки и идентификации и пр.

Работоспособность линии зависит от ряда важных электрических параметров:

— целостность соединений в цепи , связность;

—характеристический импеданс и потери обратной связи;

—погонное затухание при его распространении по линии;

—затухание переходного характера;

—задержка сигнала в канале линии связи и протяженность линии;

—сопротивление линии, при прохождении тока постоянной величины;

—емкость линии электропередачи;

—симметрия в системе электрических цепей;

—наличие электрического шума, электромагнитные наложения;

- ***1) Целостность цепи***

Проведение данной проверки помогает обнаруживать допущенные при монтаже ошибки или замыкания и обрыви в сети. Подобные ошибки нередки, поэтому такие приборы очень распространены на рынке и имеют низкую цену. Основной функцией является контроль целостности, но в ряде случаев, данные приборы имеют дополнительные возможности, которые более точно классифицируют дефекты, что позволяет быстрее устранять неисправности.

2) Характеристический импеданс (волновое сопротивление)

Как правило, данные в линии передаются в высокочастотном диапазоне, и отдельного упоминания заслуживает импеданс линии, или другими словами величина сопротивления переменному току определенной частоты. Важна неизменчивость импеданса для всего спектра частот для всей линии, так как при отражении от точки с измененным импедансом основной сигнал, будет искажаться под его влиянием

Основные причины неоднородности импеданса следующие:

—нарушение развитости при разделке кабеля около соединителей

—дефекты кабеля;

—некорректный монтаж кабеля

—нарушение технологии соединения кабелей

Подобные проблемы также могут иметь место при использовании соединительных шнуров, переходников и расщепителей низкого качества или с отсутствующими сертификатами соответствия категории.

3) Погонное затухание.

Это процесс потери сигналом мощности при его распространении в линии сети (отношение сигнала на выходе к сигналу на входе). Если в линии по средством её нарушения появляется большая неоднородность импеданса, то потери возвращённые будут не большими, так как основная энергия сигнала будет отражена от неоднородности. Например, в случае замыкания или нарушения кабеля (обрыва) обратных потерь не будет.

У некоторых рефлектометров есть функция вычисления обратных потерь на определённом отрезке линии, за счёт этого мы можем определить, есть ли на этом отрезке неоднородности которые влияют на информационный сигнал.

4) Переходное затухание.

Эта характеристика описывает то как в парах одного кабеля происходят перекрёстные наводки (отношения амплитудной характеристики информационного сигнала к амплитудной характеристики наведённого сигнала).

Проводить данное тестирование можно разными способами, для того что бы провести оценку различных характеристик кабеля. Для расчёта переходного затухания на ближнем конце линии информационный сигнал подаётся и измеряется только с одной линии для всего спектра частот. В этом случае для тестирования в одной паре сигнал по очереди подаётся на другие пары. В другом случае, измерения проводится с более серьёзным подходом. Информационный сигнал подаётся на все пары, а затем суммируется затухание.

Ясно, что переходное затухание, измеренное с обеих сторон на ближнем конце линии будет более сильным, если оно будет располагаться близко к месту подачи информационного сигнала. В современных стандартах принято проводить тестирование затухания на разных концах линии в одно и то же время.

Важно учитывать, что если переходное затухание на порядок больше погонного, то можно считать, что линия работает хорошо. Но этот параметр может оказаться не достаточным, поэтому следует так же применять в дополнении к нему параметр защищённости на линии в дальнем конце, который определяется как погонное затухание, делённое на переходное затухание на ближнем конце линии. По сути, данный параметр показывает, как амплитуда информационного сигнала в канале отличается по значению от амплитуды шумов для определённого спектра частот. Приемлемое значение переходного затухания может говорить о том, что линия симметрична, а так же что в сети отсутствуют излучения и радиопомехи.

5) Длина линии и задержка распространения сигнала.

Для обеспечения приемлемой работы на достаточно высоких скоростях важно, чтобы задержка распространения сигнала не превышала определённую и была постоянной на всех парах линии сигнала. Для того чтобы измерить длину кабеля можно воспользоваться способом рефлектометрия.

6) Зашумлённость линий передач.

Иногда высокий уровень шумов и электромагнитного излучения могут нарушить устойчивую передачу информационного сигнала в линии. Большая часть устройств для тестирования имеют в своём функционале возможность измерения уровня помех и шумов, чтобы на основе этих данных можно было проанализировать и устранить шумы. Основными источниками шума является помехи от находящегося рядом с линией

электрооборудования большой мощности, например: генераторы, светильники дневного света, моторы и т.д. Чтобы эту проблему решить можно просто перемонтировать кабель на отдалении нескольких метров от таких устройств на некоторое расстояние. В ряде случаев помехи может создавать оборудование радиопередачи, в данной ситуации потребуется дополнительное экранирование кабеля или помещение его в металлический кожух.

Подводя итог можно отметить что, характеристик кабельных линий в достатке и они имеют разное предназначение в зависимости от того что требуется. Измерительные приборы так же в большом количестве представлены на рынке. Выбор типа кабеля, нюансов монтажа и тестировочного оборудования зависит от конкретной цели и потребностей. Например, если у вас есть небольшая локальная сеть, в которой не содержатся ценные сведения, а используется она исключительно для работы, то вполне подойдёт не сложный тестер для проверки линии в случае нарушения канала связи. Однако, если есть необходимость обслуживание крупной коммерческой сети, приостановка работы в которой, может нести существенный ущерб для организации, лучше иметь более серьёзный инструмент тестирования что бы точно определить характер проблемы, локализовать её и устранить в кратчайшие сроки.

Анализаторы протоколов.

На стадии проектирования сети или же её апгрейда может возникнуть потребность в изменении характеристик канала передачи, например, интенсивность потоков информационных сигналов, задержки которые появляются на различных стадиях обработки пакетов или, возможно, отредактировать время реакции на запрос, который представляет определённую важность на данном этапе.

Такие функции могут выполнять как уже ранее рассмотренные средства мониторинга, так и интегрированные в операционную систему

программные измерители. Самым развитым, в плане мониторинга и анализа сети является анализатор протоколов. Принцип работы следующий: в сети происходит чтение потоков, разбор их на пакеты для каждого определённого сетевого протокола и последующий анализ этих пакетов. Данные анализы можно использовать для последующей обработки и использования в качестве обоснования и доказательства произведённых изменений сетевых устройств или других компонентов сети, а так же для оценивания уровня производительности сети и для поиска, а так же устранения неполадок. Чтобы можно было сделать заключение о том, действительно ли было сделано изменение, нужно выполнить анализ протоколов в изменённом состоянии и неизменённом. Реализацией анализаторов протоколов может быть как отдельный программно-аппаратный комплекс, так и *LAPTOP* с соответствующим оборудованием и ПО. Важный момент заключается в том, что ПО и оборудование должны быть такими же как существующие в топологии анализируемой сети.

Анализатор протоколов включается в сеть как простой узел. Однако одновременно с тем, что все станции в этой сети получают только адресованные ей данные, анализатор протоколов имеет свойство принимать все пакеты данных в этой сети. В состав ПО анализатора протоколов входят как основные модули, которые взаимодействуют с сетевой картой и производящие декодирование получаемых данных, так и специального программного модуля, который для каждой топологии сети уникален. Более продвинутые анализаторы протоколов могут быть использованы с экспертными системами, которые могут на основе данных анализатора выводить информацию о том, какая неисправность в сети имеет место быть и так же давать дополнительные сведения о проанализируемых результатах измерений.

Рассмотрим подробнее состав анализатора протокола и принцип его действия:

1. Графическое представление.

Многие анализаторы протоколов имеют возможность выводить данные анализа в графическом виде, то есть получать в реальном времени информацию, результаты анализа, оценку параметров производительности сети, показывать информацию о неполадках и представлять их в наглядной форме.

2. Буфер захвата.

Основной характеристикой буфера анализатора трафика – объём.

Буфер может быть реализован как аппаратно, так и программно. В первом случае он встраивается в сетевую карту, во втором случае, память для него выделяется из ОЗУ компьютера. В случае аппаратного интегрирования скорость ввода повышается многократно, однако, это очень дорогостоящий процесс. Если ресурсов будет недостаточно, есть вероятность что информация будет теряться, в таком случае анализ данных будет не эффективным. Объём буфера позволяет задать выборки рассматриваемых данных. Буфер имеет ограниченный объём и соответственно при заполнении памяти она либо начинается сначала, либо вовсе перестаёт анализировать пакеты в сети.

3. Фильтры.

Фильтры используются, когда необходимо выявлять определённые данные. Фильтр в самом простом понимании - есть условие: либо пакет соответствует условию и сохраняется в буфер захвата, либо игнорируется. Применение фильтров ускоряет процесс сбора определённых пакетов, и пропуска ненужных. Данные действия позволяют ускорять мониторинг и анализ, в некоторых случаях это время может оказаться критическим.

4. Переключатели.

Это созданные в начале тестирования условия, которые определяют рамки процесса захвата информационных данных в сети, например: задание времени начала и остановки процесса захвата, либо наличие в

собранных данных определённых значений. Для проведения более грамотного анализа совместное использование фильтров и переключателей позволяет точно ограничить выборку данных.

5. Поиск.

Анализаторы протоколов имеют возможность ускорить процесс анализа информации, которая находится в буфере, путём нахождения в нём данных соответствующих определённым значениям. В отличии от фильтров поиск работы с данными непосредственно в буфере, в то время как фильтры работают с внешним потоком информации, который подходит заданным параметрам фильтрации. Анализ может быть произведён в следующей последовательности:

—Захват данных из канала

—Чтение этих данных

—Анализированние накопленных данных

—Идентификация ошибок (в некоторых случаях по мимо идентификации ошибки анализатор протоколов может указать узел, от которого получены ошибочные пакеты)

—Тестирование производительности (вычисляется процент использования утилизации сети или среднее значение времени ответа на запрос)

—Тестирование определённых участков сети.

Как правило, весь процесс может занять от нескольких часов до одного-трёх дней. В настоящее время анализаторы протоколов могут работать одновременно с несколькими протоколами глобальных сетей, протоколами маршрутизаторов и другого сетевого оборудования. По мимо стандартных функций анализаторы протоколов могут так же мониторить сеть на предмет преобразований между протоколами, так же в их функцию входит расширенное тестирование и оценка пропускной способности сети. Чтобы соответствовать как можно большим критериям, анализаторы

протоколов могут быть применены в тестировании локальных вычислительных сетей на всех популярных и доступных в настоящее время интерфейсах. Например, самое продвинутое из таких устройств может работать с протоколами IP- телефонией или наглядно представлять все уровни модели OSI и декодировать их.

В заключении можно сказать, что современные анализаторы протоколов обнаруживают неисправности в настройках коммутаторов, сетевого оборудования, так же позволяют работать с определённым типом трафика пересылаемого по информационному каналу, указывать на источники подозрительного трафика, производить элементы тестирования, осуществлять мониторинг с фильтрованием и декодированием протоколов в любом канале, анализ собранных данных в режиме реального времени.

Свойства и характеристики протоколов мониторинга.

Протокол SNMP.

В переводе с английского - простой протокол управления сетью **.**

Этот инструмент позволяет управлять сетями связи базируясь на архитектуре TCP/IP. Данный протокол был создан, чтобы обеспечить своевременное тестирование и проверки на предмет работоспособности сетевых маршрутизаторов и мостов. С развитием информационных технологий в данный протокол вошли прочие сетевые устройства, например – хабы, шлюзы, терминальные сервера и т.д. Этот протокол по мимо мониторинга имеет функцию редактирования настроек указанных устройств.

Данный протокол должен был упростить мониторинг и управление устройствами и программным обеспечением в сети по средствам передачи информации между агентами, которые контролируют работу устройств в сети и менеджерами, которые располагаются в пунктах управления. Этот протокол разбивает сеть на отдельные элементы (узлы, маршрутизаторы, терминальные серверы, шлюзы), так же производит мониторинг и

управление каждого отдельного элемента в сети. Мониторинг осуществляется по средствам установленных на сетевом оборудовании так называемых агентов. Агент – это часть системы, которая собирает и отправляет данные мониторинга, которые были собраны на сетевом оборудовании менеджеру и тем самым позволяет осуществлять на основе этих данных управление устройством.

Агенты бывают *аппаратные* и *программные.*

Программный агент – это программа, которая может выполнять управляющие функции и собирать статистику.

Аппаратный агент – это устройство, в котором расположены программные агенты.

Данные отправляемые на сервер менеджеру хранятся в виде дерева с описанием и записываются в базы управляющей информаций. Данные базы могут быть разных типов, как правила для каждого стандарта имеется своя конкретная база. Основными стандартами для таких баз является MIB-I и MIB-II.

Рассмотрим подробнее MIB-I. В неё входит 8 групп:

—Система.

Сводные сведения об устройстве (уникальный индетификатор устройства)

—Интерфейсы.

В данной группе хранятся сведения о сетевых интерфейсах оборудования.

—Таблица перевода адреса.

Здесь записываются данные о соответствии сетевого и физического адреса.

—Интернет протокол.

Сюда записываются сведению, которые касаются протоколов IP (статистика IP пакетов, хостов, адреса IP шлюзов).

—Протокол межсетевых управляющих сообщений.

—TCP

Информация связанная с TCP.

—UDP

—Протокол внешнего шлюза.

Данные связанные с используемой информацией в сети ИНТЕРНЕТ.

Суммируя выше сказанное можно определить что MIB- I был тесно завязан на стеке протоколов TCP/IP.

В разработанном позднее MIB-II были учтены недоработки MIB-I, а так же было увеличено число групп, теперь их стало десять.

Агенты RMON.

В дополнение к *SNMP* можно использовать спецификацию RMON, которая позволяет удалённо работать с базой MIB.

RMON – это протокол осуществляющий мониторинг вычислительных сетей, которые базируются на собирании и анализе данных о свойствах информаций которые передаются в сети.

Данный протокол похож в некоторых аспектах на предыдущий *SNMP*, здесь мониторинг информации так же осуществляется программно аппаратными агентами, которые в свою очередь передают данные на компьютер, где расположены средства управления сетевыми устройствами. Однако, отличие состоит в том, что информация которая собирается в протоколе RMON фиксирует не только события не только на сетевых устройствах, где установлен агент, но и данные так или иначе показывают характеристику трафика между такими устройствами. Дополнительным преимуществом протокола RMON перед протоколом *SNMP* - что в нём есть возможность удалённого управления сетевыми устройствами. Специально созданная база управления информации имеет ряд преимуществ по сравнению с предыдущими версиями, что позволяет ускорять работу и экономить время. Что касается модулей анализа, то в них так же проведён

ряд усовершенствований в плане сбора статистики, анализа, фильтрации и установки сигналов предупреждения. Заложенные в агентов функции позволяют осуществлять действия по идентификации неисправности и нейтрализации отказов. К примеру: протокол RMON при использовании локальной сети может на протяжении, какого-то времени мониторить сеть и анализировать её функционирование, а затем, когда функционирование отклонится от определённой нормы - выдаст оповещение. Эти данные, а так же информации с журналов может помочь администратору информационной безопасности выявить неисправность и устранить её в кратчайшие сроки.

Агентами RMON являются программно аппаратные устройства, которые интегрируются на прямую в сеть, эти устройства бывают трёх видов:

—Встроенные

—Автономные

—Устройства, базирующиеся на платформе компьютера.

Встроенные устройства – это приспособления расширения сетевых устройств. Логичное использование данного модуля является его интегрированием в сетевые концентраторы, что позволяет составить карту работы сегмента сети. С одной стороны, преимущество таких устройств заключается в том, что они осуществляют мониторинг по основным группам данных и являются относительно дешёвыми, однако, это сказывается на производительности, в первую очереди в том, что задействовано малое количество групп **RMON.**

Автономные устройства – это самые совершенные из всех созданных на данный момент устройств, а так же они имеют самую большую стоимость. Такие устройства состоят из процессора, ОЗУ, специального сетевого адаптера и дополнительных элементов. Подобные модули очень компактные и быстро развертываемые. Конечно, использование таких

устройств в очень больших сетях может быть экономически не оправданными, однако для средних сетей учитывая размер и время установки может оказать хорошее влияние.

Устройства, базирующиеся на платформе компьютера – это компьютер, подключенный в сеть, на котором установлено ПО RMON. Если сравнивать с предыдущими устройствами, то устройство, базирующиеся на платформе компьютера по цене находится между встроенными и автономными устройствами, так же минусом можно считать то, что такие устройства имеют внушительные размеры, что может повлиять на сферу их применения.

RMON включает в себя 10 групп данных:

1. Статистика – данные о свойствах и характеристиках пакетов в сети и возникающих коллизиях.
2. История – данные, которые записываются с определённым шагом времени, для того чтобы отслеживать отклонения от обычной работы.
3. Оповещение – при достижении определённого порога значения, агент отправляет менеджеру оповещение или аварийный сигнал. Администратор информационной безопасности может настраивать пороговые значения и соответствующие им уведомления, так как не во всех случаях необходимо использование аварийного сигнала. При соответствующей настройки аварийный сигнал может быть отправлен в группу событий, где происходит его дальнейший анализ.
4. Хост – информация о хостах в сети, а так же их MAC – адресах.
5. Таблица главных хостов – в этой таблице содержится список, отобранный по определённой характеристике в заданный промежуток времени.
6. Матрица трафика – данные об интенсивности пакетов, трафика между каждыми двумя хостами сети, представленная в виде матрицы.

Строки в данном случае представляются упорядоченными MAC – адресами, которые являются отправителями сообщений, а столбцы - MAC – адресами получателей. Из такой матрицы можно наглядно извлечь информацию о интенсивности трафика между парой хостов и количеством ошибок, что характерно определённая нагрузка с менеджера снимается, так как сам агент формирует эту матрицу.

7. Фильтрация – здесь задаются условия отбора. Настраивать признаки пакетов можно очень гибко от отбора до создания специальных маячков, которые будут представлять из себя события, на которое можно подготовить определённую реакцию системы.

8. Захват пакетов – правила захвата пакетов. Сюда входит буфер захвата пакетов, который собирает в себе пакеты соответствующие правилам фильтра. Здесь так же может быть захвачена только часть пакета, например, определённое количество байт, позже на основе собранных данных можно провести анализ и получить данные о функционировании сети.

9. События – здесь задаются правила создания и регистрации событий. Например, можно назначить время, когда будет отправляться аварийный сигнал управляющему модулю. Когда будет начата перехватывание пакетов или алгоритм реакции на заранее предопределённые события, происходящие в сети, такие как выход за рамки пороговых значений.

10. TokenRing – здесь находятся объекты специального назначения.

Подводя итог, можно сказать, что стандарт RMON сделал большой шаг вперёд в отличие от предыдущих стандартов, которые базировались на стеке протоколов TCP/IP (MIB-1 и MIB-II). Данный стандарт будет полезен и незаменим в тех средах передачи информации вычислительных сетей, которые используют разные протоколы сетевого уровня.

4. Пример реализации динамической модели.

В организации, деятельность организации связана с продажами, настроена сеть, структура которой представлена на рисунке с соответствующими обозначениями. Данная организация пожелала остаться неназванной.

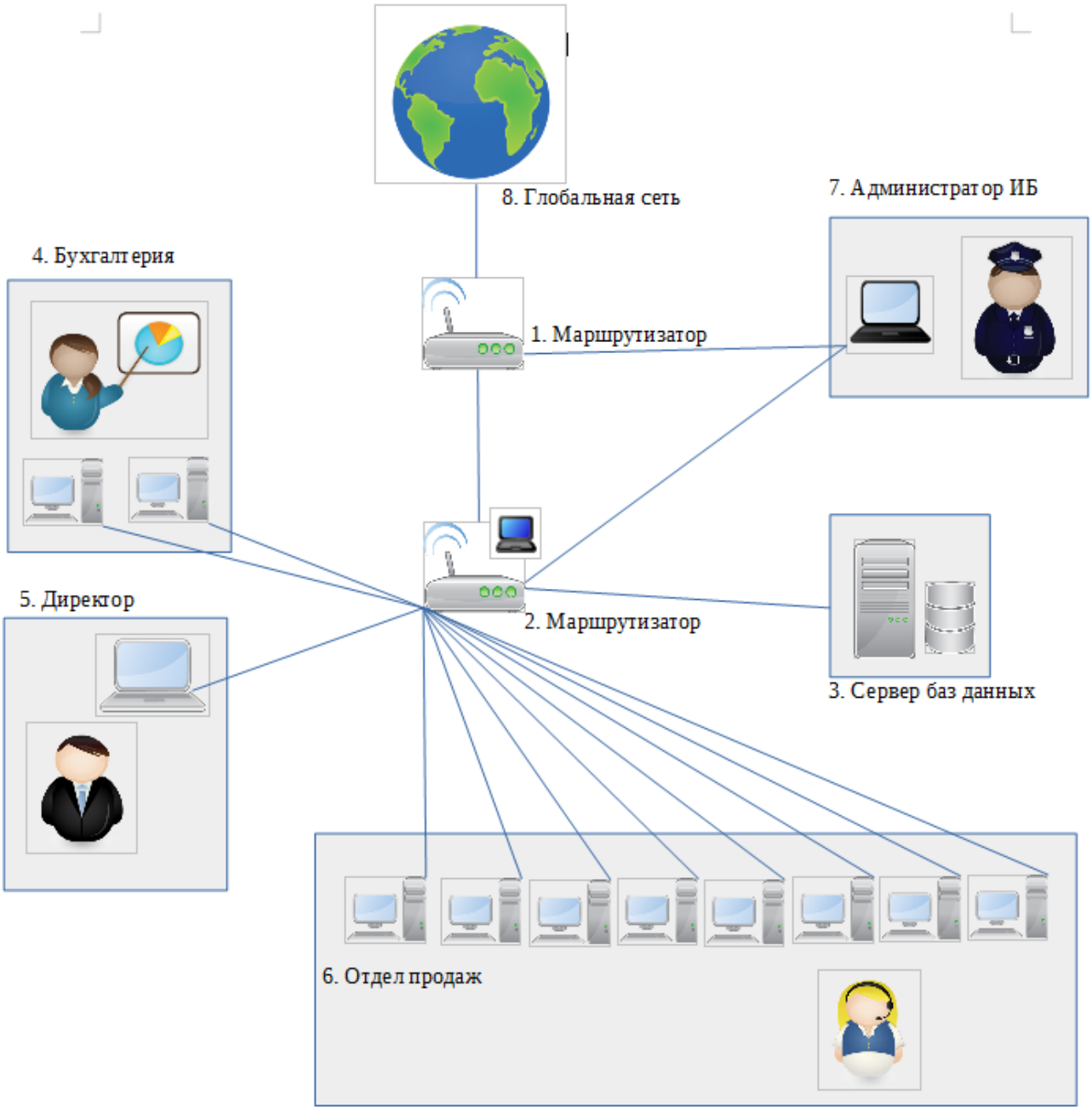

Рис. 10

Рассмотрим схему предприятия:

1. Маршрутизатор. Выполняет функцию первичного файервола, отделяет внутреннюю сеть от глобальной посредством настроенных фильтров. Имеет встроенный анализатор протоколов, который собирает статистику в сети и отправляет ее на компьютер Администратора ИБ.

2. Ширококанальный маршрутизатор с расширенными характеристиками. Обеспечивает подключение рабочих станций из бухгалтерии, кабинета директора, отдела продаж, и сервера баз данных. Также имеет функции анализа протоколов и управления.

3. Сервер баз данных. Здесь хранится вся информация и данные, необходимые для функционирования отдела продаж. На скрытом разделе жесткого диска хранятся данные, доступные только локально. Резервные копии делаются по расписанию.

4. Кабинет бухгалтера и помощника, две рабочие станции. Имеют доступ в глобальную сеть по определенному протоколу, также имеют ограниченный доступ к серверу баз данных. При работе с определенными протоколами в локальной сети, трафик во внешнюю(глобальную) сеть блокируется.

5. Кабинет директора. Одна рабочая станция с определенными полномочиями. При работе с определенными протоколами в локальной сети, трафик во внешнюю(глобальную) сеть блокируется.

6. Отдел продаж. 10 рабочих станций, на каждой установлена сетевая карта с поддержкой RMON. Имеют доступ на сервер баз данных к данным доступных для чтения и данных для редактирования. Каждой рабочей станции выделена квота дискового пространства размером 20Гб.

7. Администратор информационной безопасности. Одна рабочая станция с установленным специальным ПО для анализа данных мониторинга сети.

Требования к сети.

Табл 4

№	Критерии	Значение
1	Скорость передачи данных	До 100 Мбит/с, согласно ТТХ оборудования
2	Безопасность	Сетевой экран между внутренней сетью и внешней, ограничение доступа к настройкам оборудования, антивирусное ПО
3	Открытость	Наличие доступа во внешнюю сеть по разрешенным протоколам, фильтрация разрешенных сайтов, невозможность подключения новых устройств без контроля администратора ИБ
4	Гибкость	Свойство системы работать в условиях меняющейся структуры(выключение ПК, выход из строя сетевого устройства)
5	Эффективность	Решение всех задач в рамках первоначального бюджета, или минимально возможных затратах.

В сети осуществляется мониторинг элементов сети средствами анализаторов трафика 1 и 2, встроенный в маршрутизатор в первом случае и с реализованным программно-аппаратным комплексом во втором случае. Информация о мониторниге отправляется с этих устройств на компьютер администратора ИБ. На всех компьютерах установлена сетевая карта, имеющая полную поддержку спецификации RMON, которая отправляет данные мониторинга также администратору ИБ.

Стоит задача организовать защиту данных от подмены, нарушения уничтожения и других угроз.

Перейдем к разработке технологии управления процессом обеспечения ИБ:

Прежде всего нужно установить уровень опасности в системе в зависимости от воздействующих на нее угроз.

В нашем случае- основые угрозы есть подмена, нарушение уничтожение данных в сети и другие угрозы, нарушающие обычное функционирование сети и информационного процесса.

Следующим важным моментом является разработка методики обоснования путей снижения уровня информационной опасности до приемлемого уровня.

Выделим основные:

Настройка маршрутизаторов в соответствии с картой сети и правами доступа.

Организация постоянного непрерывного мониторинга и последующего анализа данных.

Система обеспечения безопасности может отключать подозрительные устройства внутренней сети, фильтровать протоколы, блокировать или задерживать пакеты и протоколы до принятия решения администратором ИБ.

ЛПР, в нашем случае, администратор ИБ должен на основе данных мониторинга и анализа, в случае невозможности решения проблемы системой самостоятельно разрешать их.

Эффективность реализации управленческого решения зависит от времени проявления проблемы, идентификации и нейтрализации.

На основании параметрических представлений управленческого решения, состоящих из

– «Обстановки» - $\Delta t_{\lambda}=f_{\lambda}(x_1, x_2, \ldots, x_n)$

– «Информационно–аналитической работы» $\Delta t_{v_1}=f_{v_1}(y_1, y_2, \ldots, y_m)$

– «Обеспечения субъектом реализации предназначения СОБ в соответствующей обстановке» - $\Delta t_{v_2}=f_{v_2}(z_1, z_2, \ldots, z_k)$.

Вернемся к соотношению (10)

$$P_{00}=P_{ОБСЛ}\frac{v_1 v_2}{\lambda(\lambda+v_1+v_2)+v_1 v_2}$$

Здесь видна связь всех трех параметров, которые находятся в аналитической зависимости обобщённых характеристик обстановки ($\Delta t_{пп}$), информационно-аналитической деятельности ($\Delta t_{ип}$) и нейтрализации проблемы ($\Delta t_{нп}$), возникшей при управлении безопасностью информационной системы.

При воздействии потока информационных угроз λ они анализируются посредством мониторинга и выявляют с интенсивностью ν_1 потребности в задействовании систем обеспечения безопасности.

После этого администратор информационной безопасности с периодичностью Δt (с интенсивностью ν_2) вырабатывает решение, которое гарантированно отрабатывает система обеспечения безопасности.

Обратимся к сетевому моделированию для создания наглядного представления о возможных событиях мониторинга и элементов анализа.

4.1 Синтез модели

Табл 5

Усл. обозначение	Описание события
a0	Начало мониторинга
a1	Опрос маршрутизатора 2
a2	Проверка уведомлений
a3	Сбор данных из буфера
a4	Проверка настроек
a5	Опрос маршрутизатора 1
a6	Сбор данных из буфера
a7	Проверка настроек
a8	Опрос сетевых карт устройств
a9	Проверка настроек сетевых карт устройств

а10	Запись в журнал

Перечень работ мониторинга и элементов анализа

Табл 6

Усл. Обозн работы	Описание работы	Время вып. Раб., сек	Предшествующие работы	Последующие работы
А01	Отправка Служебной команды	5	-	А12
А12	Процесс считывания данных	20	А01	А23
А23	Процесс проверки уведомлений	10	А12	А34
А34	Процесс сравнения текущих настроек с сохраненными	10	А23	А48
А410	Процесс записи данных в журнал	40	А34	-
А05	Отправка Служебной команды	5	-	А56
А56	Процесс считывания данных	20	А05	А67
А67	Процесс сравнения текущих настроек с сохраненными	10	А56	А78
А710	Процесс записи данных в журнал	40	А67	-
А08	Отправка Служебной команды	60	-	А910
А89	Процесс сравнения текущих настроек с сохраненными	60	А08	А910
А910	Процесс записи данных в журнал	60	А89	-

Проанализируем сетевой график мониторинга сети и вычислим наиболее раннее возможное время наступления j-го события T_p (j), вычисляемое по формуле:

$$T_P(j)=\frac{\max}{i\subset j}(T_P(i)-t_{ij})$$, где

- i и j обозначаются номера предшествующего и последующего событий соответственно;

- t_{ij} — продолжительность (i, j) -й работы.

Из обозначения $i\subset j$ следует, что событие i предшествует событию j.

Табл 7

$T_p(0)=0$	$T_p(6)=5+20=25$
$T_p(1)=0+5=5$	$T_p(7)=25+10=35$
$T_p(2)=5+20=25$	$T_p(8)=0+60=60$
$T_p(3)=25+10=35$	$T_p(9)=60+60=120$
$T_p(4)=35+10=45$	$T_p(10)=120+60=180$
$T_p(5)=0+5=5$	

Так как сетевой график имеет линейные ветки, самое раннее и самое позднее время наступления события совпадают.

Резерв времени данного события Ri вычисляемый по формуле

$$R_i=(T_П(i)-T_P(i))$$

и Полный резерв времени работы rп (i,j), вычисляемый по формуле

$$r_П(\mathrm{i,j})=(T_П(j)-T_P(i)-t_{ij})$$

будет равен

Табл 8

$T_p(01)=80$	$T_p(56)=50$
$T_p(12)=6$	$T_p(67)=40$
$T_p(23)=50$	$T_p(710)=0$
$T_p(34)=40$	$T_p(08)=120$
$T_p(410)=0$	$T_p(89)=60$
$T_p(05)=70$	$T_p(910)=0$

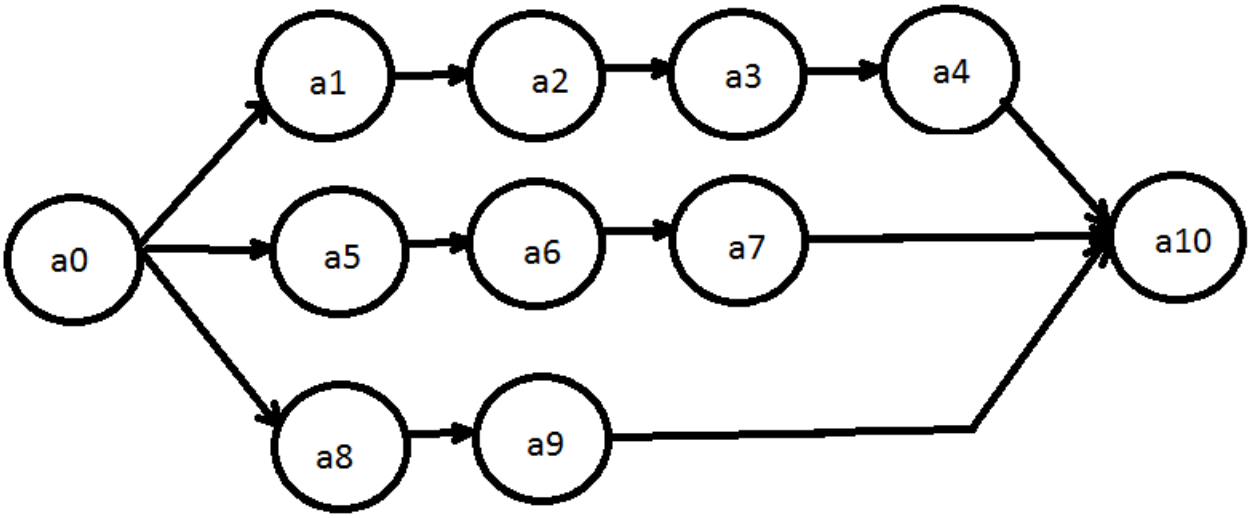

Рис 11

Обратимся к сетевому моделированию для создания наглядного представления о возможных событиях устранения проблемы

Табл 9

Усл. обозначение	Описание события
z1	Обнаружена проблема
z2	Чтение журнала тестирования
z3	Проблема М1
z4	Оборудование не отвечает

z5	М1 некорректные настройки оборудования
z6	М1 сомнительный трафик(шифрованный)
z7	М1 превышен порог подозрительная активность
z8	Оповещение администратора ИБ
z9	Изменение настроек в соответствии с сохраненными
z10	Временное блокирование клиента в сети, оповещение администратора ИБ
z11	Ограничение работы по протоколу с сомнительным трафиком, оповещение администратора ИБ
z12	Проблема М2
z13	М2 превышен порог подозрительная активность
z14	М2 сомнительный трафик(шифрованный)
z15	М2 некорректные настройки оборудования
z16	Оборудование не отвечает
z17	Ограничение работы по протоколу с сомнительным трафиком, оповещение администратора ИБ
z18	Временное блокирование клиента в сети, оповещение администратора ИБ
z19	Изменение настроек в соответствии с сохраненными

z20	Оповещение администратора ИБ
z21	Проблема сетевое устройство
z22	Некорректные настройки сетевых устройств
z23	Изменение настроек в соответствии с сохраненными, оповещение администратора ИБ
z24	Уникальный идентификатора сетевого устройства не соответствует базе доверенных устройст
z25	Блокировка любого трафика в сети, оповещение администратора ИБ
z26	Корреляция z11 z17
z27	Корреляция z10 z18
z28	Корреляция z9 z19
z29	Запись в журнал

Перечень работ устранения проблем

Табл 10

Усл. Обозн работы	Описание работы	Время вып. Раб., сек	Предшествующие работы	Последующие работы
1-2	Выполнение чтения журнала тестирования	1	-	2-3,2-12, 2-21
2-3	Переход к решению проблемы для М1	3	2-1	3-4,3-5,3-6,3-7

2-12	Переход к решению проблемы для М2	3	2-1	12-13,12-14,12-15, 12-16
2-21	Переход к решению проблем для сетевых устройств	3	2-1	21-22, 21-24
3-4	Выявлена проблема М1: оборудование не отвечает	5	2-3	4-8
3-5	Выявлена проблема М1: некорректные настройки оборудования	5	2-3	5-9
3-6	Выявлена проблема М1: сомнительный трафик(шифрованный)	2	2-3	6-10
3-7	Выявлена проблема М1: превышение порога	1	2-3	7-11
4-8	Отправка уведомления администратору ИБ	1	3-4	8-29
5-9	Выполнение изменения настроек оборудования	20	3-4	9-28
6-10	Выполнение блокировки клиента и отправка уведомления администратору ИБ	1	3-4	10-27
7-11	Выполнение фильтрации трафика с его последующим сохранением и отправка уведомления администратору ИБ	1	3-4	11-26

12-13	Выявлена проблема М2: превышение порога	1	2-12	13-17
12-14	Выявлена проблема М2: сомнительный трафик(шифрованный)	2	2-12	14-18
12-15	Выявлена проблема М2: некорректные настройки оборудования	5	2-12	15-19
12-16	Выявлена проблема М2: оборудование не отвечает	5	2-12	16-20
13-17	Выполнение фильтрации трафика с его последующим сохранением и отправка уведомления администратору ИБ	1	12-13	17-26
14-18	Выполнение блокировки клиента и отправка уведомления администратору ИБ	1	12-14	18-27
15-19	Выполнение изменения настроек оборудования	20	12-15	19-28
16-20	Отправка уведомления администратору ИБ	1	12-16	20-29
21-22	Выявлена проблема сетевого оборудования: некорректные настройки сетевых устройств	30	2-21	22-23
21-24	Выявлена проблема сетевого оборудования: некорректный	5	2-21	24-25

	идентификатор сетевого устройства			
22-23	Выполнение изменения настроек сетевого оборудования	20	21-22	23-29
24-25	Выполнение полной блокировки устройсва, обовещение администратора ИБ	1	21-24	25-29
9-28	Выявление взаимосвязей некорректных настроек с сохраненными данными	10	5-9	28-29
19-28	Выявление взаимосвязей некорректных настроек с сохраненными данными	10	15-19	28-29
10-27	Выявление взаимосвязей текущего трафика и сохраненного	10	6-10	27-28
18-27	Выявление взаимосвязей текущего трафика и сохраненного	10	14-18	27-28
11-26	Выявление взаимосвязей превышенных порогов с сохраненными данными	10	7-11	26-27
17-26	Выявление взаимосвязей превышенных порогов с сохраненными данными	10	13-17	26-27
8-29	Запись данных в журнал	5	4-8	-
28-29	Выполнение анализа данных и запись в журнал	5	9-28, 27-28, 19-	-

			28	
20-29	Запись данных в журнал	5	16-20	-
23-29	Запись данных в журнал	5	22-23	-
25-29	Запись данных в журнал	5	24-25	-
26-27	Выявление взаимосвязей сомнительного трафика и нарушенных порогов активности	10	11-26, 17-26	27-28
27-28	Выявление взаимосвязей 26-27, а также некорректных настроек оборудования	10	10-27, 26-27, 18-27	28-29

Анализ сетевого графика устранения пробемы

Основными параметрами сетевого графика являются:

1. Наиболее раннее возможное время наступления j-го события T_p (j), вычисляемое по формуле:

$$T_P(j)=\max_{i\subset j}(T_P(i)-t_{ij})$$, где

- i и j обозначаются номера предшествующего и последующего событий соответственно;

- t_{ij} — продолжительность (i, j) -й работы.

Из обозначения $i\subset j$ следует, что событие i предшествует событию j.

Табл 12

$T_p(1)=0$	$T_p(11)=6$	$T_p(21)=4$
$T_p(2)=1$	$T_p(12)=4$	$T_p(22)=34$
$T_p(3)=4$	$T_p(13)=5$	$T_p(23)=54$
$T_p(4)=9$	$T_p(14)=6$	$T_p(24)=9$

$T_p(5)=9$	$T_p(15)=9$	$T_p(25)=10$
$T_p(6)=6$	$T_p(16)=9$	$T_p(26)=16$
$T_p(7)=5$	$T_p(17)=6$	$T_p(27)=17$
$T_p(8)=10$	$T_p(18)=7$	$T_p(28)=27$
$T_p(9)=29$	$T_p(19)=29$	$T_p(29)=15$
$T_p(10)=7$	$T_p(20)=10$	

2. Самое позднее допустимое время наступления i-го события Тп (i), вычисляемое по формуле

$$T_П(j)=\min_{i\supset j}(T_П(i)-t_{ij})$$

где из обозначения $i\supset j$ следует, что событие j предшествует событию i

Табл 13

$T_p(1)=0$	$T_p(11)=6$	$T_p(21)=4$
$T_p(2)=1$	$T_p(12)=4$	$T_p(22)=34$
$T_p(3)=4$	$T_p(13)=5$	$T_p(23)=54$
$T_p(4)=9$	$T_p(14)=6$	$T_p(24)=9$
$T_p(5)=9$	$T_p(15)=9$	$T_p(25)=10$
$T_p(6)=6$	$T_p(16)=9$	$T_p(26)=16$
$T_p(7)=5$	$T_p(17)=6$	$T_p(27)=26$
$T_p(8)=10$	$T_p(18)=7$	$T_p(28)=39$
$T_p(9)=29$	$T_p(19)=29$	$T_p(29)=59$
$T_p(10)=7$	$T_p(20)=10$	

3. Резерв времени данного события Ri вычисляемый по формуле

$$R_i=(T_П(i)-T_P(i))$$

$T_p(1)=0$	$T_p(11)=0$	$T_p(21)=0$
$T_p(2)=0$	$T_p(12)=0$	$T_p(22)=0$
$T_p(3)=0$	$T_p(13)=0$	$T_p(23)=0$
$T_p(4)=0$	$T_p(14)=0$	$T_p(24)=0$
$T_p(5)=0$	$T_p(15)=0$	$T_p(25)=0$
$T_p(6)=0$	$T_p(16)=0$	$T_p(26)=0$
$T_p(7)=0$	$T_p(17)=0$	$T_p(27)=9$
$T_p(8)=0$	$T_p(18)=0$	$T_p(28)=12$
$T_p(9)=0$	$T_p(19)=0$	$T_p(29)=44$
$T_p(10)=0$	$T_p(20)=0$	

4. Полный резерв времени работы $r_п$ (i,j), вычисляемый по формуле

$$r_П(\mathrm{i,j})=(T_П(j)-T_P(i)-t_{ij})$$

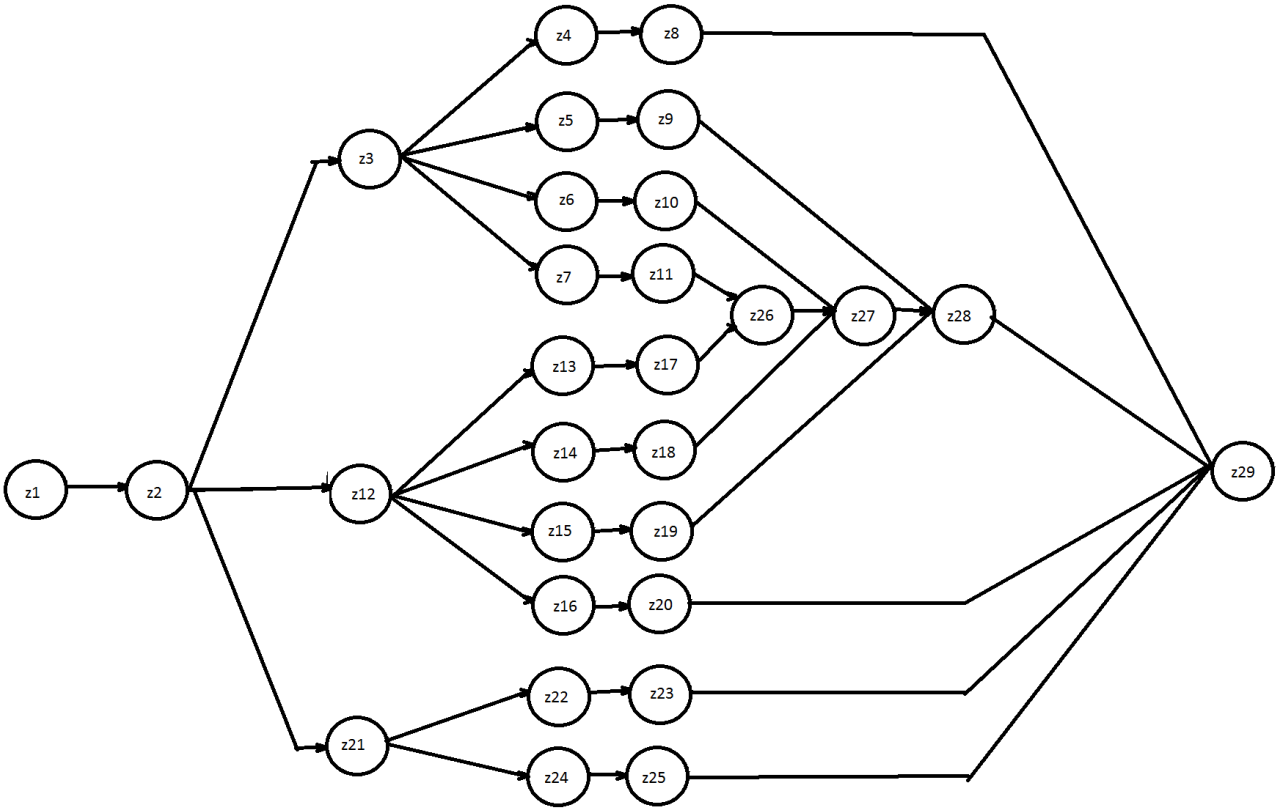

Рис. 12 Сетевой график устранения проблемы

1. Критический путь мониторинга сети:

   a0-a8-a9-a10

   $T_{кр}$==180 сек

2. Критический путь устранения проблем:

   z1-z2-z21-z22-z23-z29

   $T_{кр}$==59 сек

Расчеты при полученных данных

$\Delta t_{нп}$ = 0,5 (час)=1800 (сек); λ=0,00055

$\Delta t_{ип}$ = 180 (сек); ν_1=0,0055

$\Delta t_{нп}$ = 59 (сек); ν_2=0,0169

Используя эти данные и произведя расчеты по формуле

$P_{00} = \frac{\nu_1 \nu_2}{\lambda(\lambda + \nu_1 + \nu_2) + \nu_1 \nu_2}$, получим вероятность, равную **0.88**

Рассчитаем среднее время проявления проблемы в системе (λ) для заданных вероятностей: 0.8, 0.9.

Для вероятности P_{00}=0,8 среднее время проявления проблемы должно быть 1010 сек или 17 минут.

Для вероятности P_{00}=0,9 среднее время проявления проблемы должно быть 2222 сек или 37 минут.

4.2Вывод:

Информационная безопасность для данного предприятия очень важна, поэтому нужно соблюсти системную интеграцию процессов:

— проявления проблемы

— распознавания проблемы

— профилактики проблемы

Для достижения данного результата необходимо:

Уменьшить время нейтрализации проблемы и\или ускорить процесс мониторинга. Достичь этого можно путем оптимизации начальных фильтров, настроек и их последующем использовании в динамической системе. Жесткие рамки процессов позволят быстрее анализировать результаты мониторинга.

Применяя современные программно-аппаратные средства совместно с существующими технологиями можно также существенно повысить уровень безопасности.

В данном рассмотренном случае применяются современные средства мониторинга, жесткие рамки политики безопасности и подсистема автоматического реагирования на очевидные случаи возникновения неисправностей. Для обеспечения работоспособности локальной вычислительной сети, в сложном случае, в автоматическом режиме обеспечиваются меры по смягчению обстоятельств до принятия мер по нейтрализации проблемы администратором информационной безопасности.

Заключение.

Развитие новых технологий порождает новые информационные системы, которые становятся только сложнее по своей структуре и требуют повышенного внимания к обслуживанию. Информация, представленная в виде данных, может иметь значение как для отдельной личности, так и для целых государств. Защита таких данных является важной необходимостью, ведь потенциальные потери от нарушения целостности, конфиденциальности или доступности таких данных могут быть весьма существенными.

Если подходить к вопросу системно, то нужно методично и грамотно строить защиту, используя все известные методы. Однако существующая проблема несоответствия угроз реальным рискам остается под вопросом.

Получить гарантированный результат позволяют динамические системы, модель работы которых мы рассмотрели.

Список использованной литературы:

1. Бурлов В.Г. Логико-алгебраическая концепция построения модели системы и её приложение для синтеза системы защиты информации (в кн. «Безопасность информации регионов России») НТК 13-15. 10. 1999 г.- СПб.; СПИИРАН, 1999.

2. Бурлов В.Г. Методы построения систем поддержки принятия решения, основанные на логико - алгебраической системной концепции математики. (Тезисы доклада) НТК 28-29 10, - С-Пб; ВИКУ им. А.Ф. Можайского, 1999.

3. ГОСТ Р 52448-2005 «Национальный стандарт Российской Федерации. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.» Введ. С 01.01.07 ГНИИИ ПТЗИ ФСТЭК России

4. ГОСТ Р 51344-99 «Государственный стандарт Российской Федерации. Безопасность машин. принципы оценки и определения риска.» Введ. С 01.07.00 ОАО "ЭНИМС"

5. ГОСТ Р 51901.1-2002 «Государственный стандарт Российской Федерации. Менеджмент риска. (поправка. иус 8-2005 г.). Анализ риска технологических систем. Госстандарт России» Введ. 07.06.02 АО НИЦ КД

6. Веб-сайт NVD Complete Vulnerability Listing, https://nvd.nist.gov/full_listing.cfm

7. Бурлов В.Г. Основы моделирования социально – экономических и политических процессов (Методология. Методы), СПБГПУ. 2006 г. –270 с., 2007.

8. Гайдамакин Н.А. Теоретические основы компьютерной безопасности, *УрГУ* .-212с. 2008.

9. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2010. - 336 с.

10. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 с.

11. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 - Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. - М.: ГЛТ, 2006. - 536 с.

12. Васильков, А.В. Информационные системы и их безопасность: Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. - М.: Форум, 2013. - 528 с.

13. Девянин, П.Н. Безопасность управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2010. - 176 с.

14. Емельянов, С.В. Труды ИСА РАН: Системы управления и моделирование. Динамические системы. Управление рисками и

безопасностью. Методы и модели в экономике. Прикладные а / С.В. Емельянов. - М.: Красанд, 2014. - 124 с.

15. Ерохин, В.В. Безопасность информационных систем: учеб пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. - М.: Флинта, 2016. - 184 с.

16. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

17. Гаранин М.В., В.И. Журавлев, С.В. Кунегин Системы и сети передачи информации Издательство: Экзамен, 336 стр., 2003 г.

18. Когаловский М.Р. Перспективные технологии информационных систем Издательства: ДМК Пресс, Компания АйТи; 288 стр., 2003 г.

19. Мизин И.А., Богатырев В.А.,Кулешов А.П. Сети, коммуникации пакетов/Под ред.В.С.Семенихина-М.:Радиосвязь,2001.

20. Бородакий, Ю.В. Информационные технологии. Методы, процессы, системы / Ю.В. Бородакий, Ю.Г. Лободинский. - М.: ГЛТ , 2004. - 456 с.

21. Гвоздева, В.А. Информатика, автоматизированные информационные технологии и системы: Учебник (ГРИФ) / В.А. Гвоздева. - М.: Форум, 2011. - 544 с.

22. Голицына, О.Л. Информационные технологии: Учебник / О.Л. Голицына, Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - М.: Форум, ИНФРА-М, 2013. - 608 с.

23. Емельянов, С.В. Информационные технологии и вычислительные системы: Интернет-технологии. Математическое моделирование. Системы управления. Компьютерная графика / С.В. Емельянов. - М.: Ленанд, 2012. - 96 с.

24. Коноплева, И.А. Информационные технологии. / И.А. Коноплева, О.А. Хохлова, А.В. Денисов. - М.: Проспект, 2015. - 328 с.

25. Логинов, В.Н. Информационные технологии управления: Учебное пособие / В.Н. Логинов. - М.: КноРус, 2013. - 240 с.

26. Петраков, А.В. Защитные информационные технологии аудиовидеоэлектросвязи / А.В. Петраков. - М.: Радио и связь, 2010. - 616 с.

27. Федоров, И.Б. Информационные технологии в радиотехнических системах / И.Б. Федоров. - М.: МГТУ , 2011. - 846 с.

28. Гончаренко, Л.П. Управление безопасностью / Л.П. Гончаренко. - М.: КноРус, 2010. - 272 с.

29. Черешкин, Д.С. Управление рисками и безопасностью / Д.С. Черешкин. - М.: Ленанд, 2010. - 200 с.

30. Овчинников, В.В. Управление безопасностью / В.В. Овчинников. - М.: КноРус, 2013. - 272 с.

31. Емельянов, С.В. Труды ИСА РАН: Алгоритмы. Решения. Математическое моделирование. Управление рисками и безопасностью / С.В. Емельянов. - М.: Ленанд, 2014. - 102 с.