МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра Телекоммуникационных систем

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой
к.т.н., профессор
Байкенов А. С.
«____» _____ 2015 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

на тему: Исследование моделей повышения производительности пакетных сетей с учетом угроз информационной безопасности

Специальность 5В071900 Радиотехника, электроника и телекоммуникации

Выполнил магистрант гр. МТСп–13–1 _____ Жаугашаров Е.А.
(подпись) (Ф.И.О.)

Научный руководитель к.т.н, профессор _____ Байкенов А.С.
(ученая степень, звание) (подпись) (Ф.И.О.)

Консультант по ВТ к.т.н, старший преподаватель _____ Ефремова Ю.И.
(ученая степень, звание) (подпись) (Ф.И.О.)

Нормоконтролер магистр, ассистент _____ Зайцев Е.О.
(ученая степень, звание) (подпись) (Ф.И.О.)

Рецензент к.т.н., доцент _____ Орынбет М.М.
(ученая степень, звание) (подпись) (Ф.И.О.)

Алматы, 2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет «Радиотехники, электроники и связи»

Кафедра «Телекоммуникационных систем»

Специальность 6М071900 «Радиотехники, электроники и телекоммуникации»

ЗАДАНИЕ
на выполнение магистерской диссертации

Магистранту Жаугашарову Ерболу.

Тема диссертации Исследование моделей повышения производительности пакетных сетей с учетом угроз информационной безопасности

Утверждена приказом по университету № 17 от «12» декабря 2014 г.

Срок сдачи законченного диссертации «_____» _____201___г.

Перечень вопросов, подлежащих разработке в магистерской диссертации, или краткое содержание магистерской диссертации: предложена имитационная модель систем повышения производительности пакетных сетей с учетом угроз информационной безопасности.

Перечень графического материала (с точным указанием обязательных чертежей):

1 Вероятность достоверного обнаружения ВТ сенсорами IDS при разных алгоритмах обнаружения;

2 Средняя задержка пакета в сети при включенной и выключенной СЗИ;

3 Вероятность «ложной тревоги» сенсоров IDS при различно степени нагрузки на сеть.

Основная рекомендуемая литература:

1. Алешин, Л.И. Защита информации и информационная безопасность / Л.И. Алешин. -М.: МГУК, 1999. - 176 с.

2. Артемов, Д.В. Влияние компьютерных вторжений на функционирование вычислительных сетей / Д.В. Артемов. - М: Приор, 2001. - 123 с.

График
подготовки магистерской диссертации

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1 Проблема производительности пакетных сетей. Анализ объекта исследования	30.09.13 г.	
2 Разработка и исследование аналитических моделей оценки производительности пакетной сети	15.10.13 г.	
3 Разработка и исследование моделей повышения производительности пакетной сети	07.01.14 г.	
4 экспериментальные исследования производительности пакетной сети	15.10.14 г.	
5 Анализ результатов эксперимента	10.11.14 г.	

Дата выдачи задания «___» _____ 201___г.

Заведующий кафедрой _____ Байкенов А. С.
(подпись) (Ф.И.О.)

Руководитель диссертации _____ Байкенов А. С.
(подпись) (Ф.И.О.)

Задание принял к исполнению
магистрант _____ Жаугашаров Е.А.
(подпись) (Ф.И.О.)

Аңдатпа

Бұл жұмыс пакеттік желілердің ақпараттық қауіпсіздікке қатер төнген кездегі жылдамдықтың азаюына байланысты мәселені қарастырады . Пакеттік желінің аналитикалық және имитациялық моделдері зерттелді. Кідірістің,шығынның және өткізу қабілетінің мәнін анықтау мақсатында желі жұмысының аналитикалық және имитациялық моделдері көрсетілген. Аналитикалық және имитациялық моделдеудің нәтижелері салыстырылды.

Аннотация

Работа посвящена проблеме повышения производительности пакетной сети в условиях воздействия угроз информационной безопасности. Было проведено исследование аналитический и имитационных моделей пакетных сетей. Представлены алгоритмы обнаружения вредоносного потока с целью определения значений задержки, потери и пропускной способности. Проведено сравнение результатов аналитического и имитационного моделирования.

Annotation

This work is devoted to increasing of productivity of the packet switching networks in condition of information security threat . The study was conducted analytical and simulation models of packet switching network. The analytical and simulation models of the work site in order to determine the values of delay, loss and bandwidth. Comparison of results of analytical and imitation design is conducted.

Содержание

Введение.....6
1 Проблема производительности пакетных сетей. Анализ объекта исследования.....9
1.1 Общая структура пакетных сетей.....10
1.2 Показатели производительности пакетной сети.....13
1.3 Причины снижения производительности пакетной сети.....15
1.4 Уточнение задачи исследования.... **Ошибка! Закладка не определена.**23
2 Разработка и исследование аналитических моделей оценки производительности пакетной сети.....25
2.1 Замкнутая модель пакетной сети.....25
2.2 Разомкнутая модель пакетной сети.....33
3 Разработка и исследование моделей повышения производительности сети.40
3.1. Структурная модель системы защиты информации пакетной сети.....40
3.2 Модели организации защитных механизмов в пакетной сети.....42
4 Экспериментальные исследования производительности пакетной сети.....56
4.1. Разработка экспериментальной установки пакетной сети.....57
4.2. Результаты и анализ экспериментальных исследований.....57
Заключение.....62
Список литературы.....63
Приложение А.....65
Приложение Б.....66

Введение

Сети с пакетной коммутацией со временем все больше замещают сети с коммутацией каналов, трафик этих сетей растет с геометрической прогрессией, и поэтому встает вопрос об увеличении их производительности. Усложняется структура и размеры пакетных сетей, и так же требует повышения уровня информационной безопасности.

Анализ сетей с пакетной коммутацией показывает, что значительное падение характеристик производительности происходит из-за угроз информационной безопасности, которые могут полностью заблокировать сеть. Эффективное проектирование и эксплуатация пакетных сетей, работающих в условиях угроз информационной безопасности, возможна при наличии моделей и алгоритмов, позволяющие обеспечивать требуемый уровень производительности. Модели сетей с пакетной коммутацией с использованием аппарата теории массового обслуживания предложенные Вишневским В.М. и Герасимовым А.И. не учитывают параметры угроз информационной безопасности и систем защиты. Работы предложенные Столингсом В., Норкаттом С., Касперски К., обеспечивают существенное повышение безопасности сети с коммутацией пакетов, но не обеспечивают должного уровня производительности.

Делаем вывод, то что исследование моделей повышения производительности в условиях воздействия угроз информационной безопасности является актуальным. Объект исследования – сеть с пакетной коммутацией.

Цель работы – исследование моделей повышения производительности пакетных сетей с учетом воздействия угроз информационной безопасности.

Для достижения поставленной цели в работе решены задачи:

- Анализ и выявление угроз информационной безопасности, вызывающих значительное падение характеристик производительности пакетной сети.
- Анализ моделей оценки производительности пакетной сети в условиях воздействия угроз ИБ.
- Исследование алгоритмов достоверного обнаружения угроз информационной безопасности в пакетной сети.
- Экспериментальное исследование имитационной модели с целью получения характеристик производительности пакетной сети с учетом воздействия и противодействия угрозам информационной безопасности.

1 Проблема производительности пакетных сетей. Анализ объекта исследования

Проблемы производительности телекоммуникационных сетей изучаются с 70-х годов прошедшего века и, хотя получены фундаментальные методические и теоретические результаты [1], далеко не все проблемы оценки производительности сетей можно полагать удачно разрешенными.

Становление сеток с коммутацией пакетов [2], постоянно увеличивающаяся надобность в повышении значения информационной защищенности сеток [3] дали почву увеличению задач оценки производительности пакетной сети. Специфики пакетной сети, состоят в том, собственно она обслуживает очень большое количество сетевых компонентов: серверов, коммутаторов, находящиеся на удалении друг от приятеля. При всем при этом серверы, коммутаторы, каналы имеют разные функции. Потому, неувязка оценки производительности пакетной козни состоит в том, будто большая количество разных узлов объединяются в текстуры пакетной козни разными способами.

Иная неувязка оценки производительности пакетной козни ориентируется трафиком перегрузки. В функционирующей пакетной козни трафик, его свойства ориентируются как деловитостью компании, необъективными чертами юзеров, этак и опасностями информационной сохранности, которые при собственной реализации творят доп вредный трафик (ВТ) в козни. 3-я неувязка состоит в неимении нормативно-справочной базы сообразно сетевым чертам узлов пакетной козни и сетевым характеристикам стандартных трафиков пакетной козни. Действенная эксплуатация пакетной козни, функционирующих в критериях действия опасностей информационной сохранности, их конструирование и модернизация никак не вероятны в отсутствии оценок свойства функционирования, одной из каких считается продуктивность пакетной козни.

В главерассматривается структурапакетной сети, анализируются показатели ее производительности, выявляютсясущественные угрозы информационной безопасности,вызывающие снижение ее производительности,анализируются современные способыисредства обнаруженияугроз ИБ, степень их воздействияна производительность пакетной сети. Уточняется задачасследования.

1.1 Общая структура пакетных сетей

Сеть с коммутацией пакетов предназначенная для предоставления единого защищенного сетевого пространства ограниченному рамками предприятия кругу пользователей. Обобщенная структурная схема пакетной сети приведена на рисунке 1.1. Ее состав в общем случае образуют следующие функциональные элементы:

- рабочие станции. На рисунке показаны хосты (PC), соединенные ЛВС, или выделенные рабочие станции, включающиемодулизащиты (МЗ);

- серверы (С) с разной функциональностью. Им предоставляется возможность быть сосредоточенными или распределенными на местности компании;

- средства телекоммуникационного взаимодействия обеспечения между собой рабочих станций и их взаимодействия с информационными серверами. В корпорации может быть выбран (или арендован), быть аксессуаром корпорации и общей целью (сеть связи, существующая из корпорации, которые используются предприятием);

- телеслужбы. Обмен информацией предприятия может быть понят в одном (телефония, телетекст, видеотекст, телефакс), или несколько служб (интеграция служб);

- система управления отдачей функционирования пакетной козни. В зависимости от реализуемого комплекта служб в пакетной козни употребляются собственные средства управления сетью, в частности средства маршрутизации, коммутации и администрирования, реализуемые с целью действенного применения сетевых ресурсов. Сообразно способности управления веществами пакетной козни разрешено отметить контролируемые многофункциональные составляющие (наверное личные, либо особо вводимые в рамках пакетной козни средства) и неуправляемые многофункциональные составляющие, (в частности, маршрутизаторы- и коммутаторы), являющиеся приспособлением применяемых компанией субсетей всеобщего назначения;

- система управления безопасностью пакетной сети;

- система снабжения прочности пакетной козни. Учитываются средства снабжения трудоспособности всей системы, или ее фрагментов при отказах частей пакетной козни;

- система диагностики и контролирования. В рамках пакетной козни учитываются средства контролирования трудоспособности отдельных многофункциональных частей, система сбора инфы о отказах и сбоях и

предоставления ее системам снабжения живучести; управления отдачей функционирования; управления сохранностью.

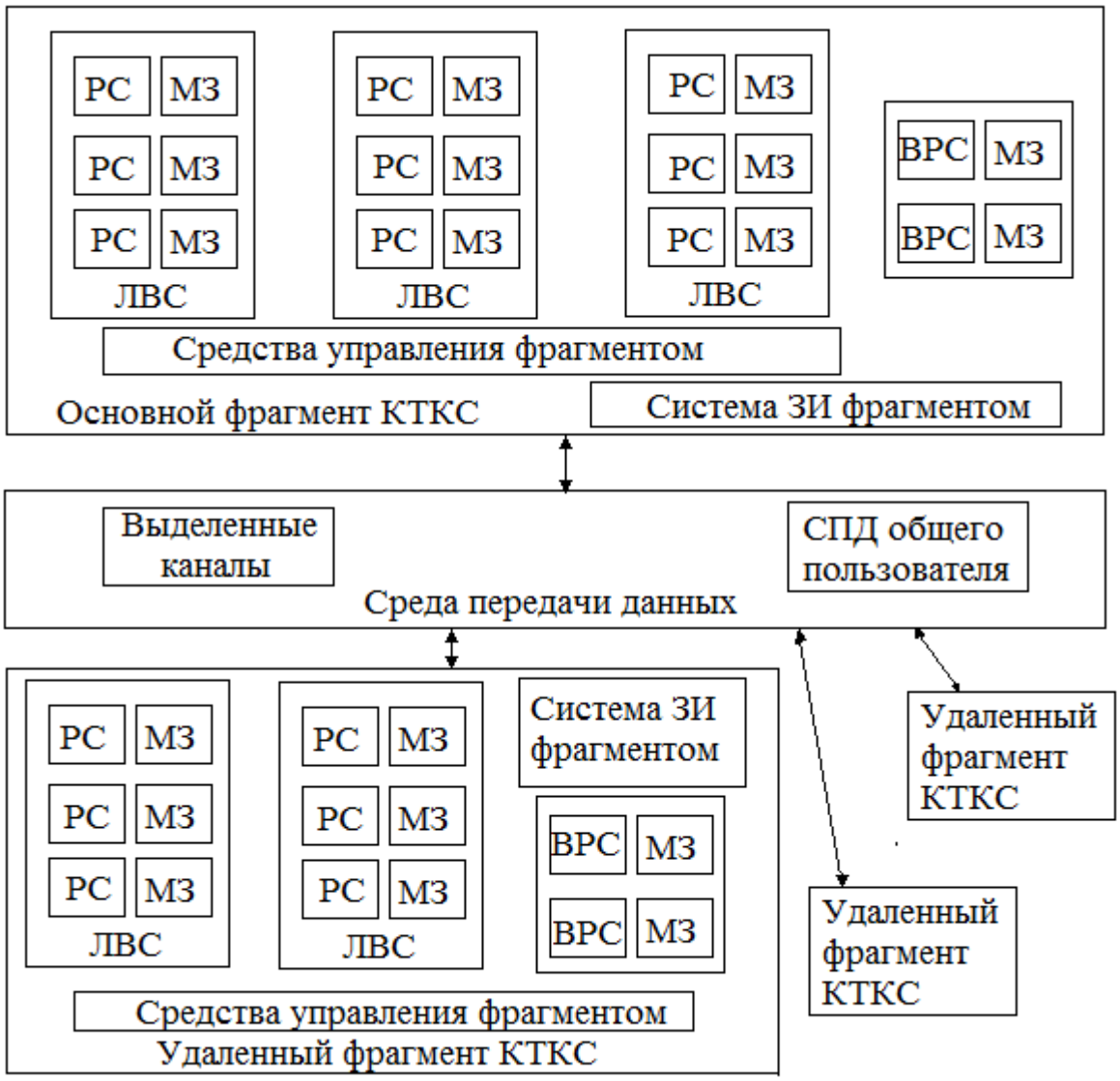

Рисунок 1.1- Обобщенная структурная схема пакетной сети

Фактически неважно какая пакетная сеть охватывает фрагменты больше обобщенной текстуры. Тут совместный вариант иллюстрирует, в котором изначальная конструкция и фрагменты дистанционного схожи. Как верховодило, данные фрагменты имеют разную сложность. Облегчение текстуры козни с коммутацией пакетов считается понижение трудности отдаленных фрагменты, надлежащие передаточные функции на деталях главного фрагмента, кой проходит в первую очередьдляследующих частей:

- информационные серверы (с точки зрения поддержки информационной безопасности сети владеет значение сосредоточить все

информационные серверы, обеспечивая для их нужную охрану организационными и техническими событиями);

- администрирование всех многофункциональных системных групп, доп ограниченное количество применяющее лекарство реализации многофункциональных системных групп (к примеру, трассировщиков) имеет возможность существовать сконцентрировано в главном фрагменте;

-включение к доступным сервисам (сеть Веб) исполняется с выделенных трудящихся мест главного фрагмента (тут употребляются надлежащие средства охраны, включения к массовым сетками в едином случае хорошие от других).

Тест обычных и платных телекоммуникационных сеток [4] указывает последующие индивидуальности пакетной козни, являющейся главной для изучения:

- обширное внедрение ОС Microsoft Windows и Unix/Linux – схожих при исследованию серверов и контроллеров. И желая изготовители ОС непрерывно улучшают собственные технологии, уязвимости в их появляются непрерывно. К примеру, в 2007 году было опубликовано возле 20 предостережений о угрозы для товаров фирмы Microsoft. Таковая ведь обстановка имеется и в отношении Unix/Linux-схожих систем;

внедрение в прикладных задачах контроллерах и серверах протоколов HTTP, SNMP, FTP, DHCP, OPC, DCOM, ActiveX, Java. Наверное дозволяет достигать большей функциональности пакетной козни, однако и привносит новейшие уязвимости в систему;

- внедрение фактически беззащитных протоколов Ethernet и TCP/IP (Modbus/TCP, EtherNet/IP, PROFInet и др.) в качестве главных операцй взаимодействия информационных действий пакетной козни;

- циркулирует информация 3-х типов: официальная (распределение которой официально санкционируется на уровне организации), массовая (специализирована для применения отдельной категорией служащих, как верховодило, подлежит охране) и неофициальная (собственная папка либо каталог на сервере). Доступ к инфы предоставляется урезанной группе покупателей и действий;

- присутствие централизованной системы управления (отдачей функционирования, сохранностью, живучестью) пакетной козни;

- неразделимость прибавлений от многофункциональных подразделений компании, так как дробь прикладных программ размещается на станции-покупателе;

- надобность одновременного контролирования нескольких локальных вычислительных сеток;

- просторный диапазон применяемых методик представления, сохранения и передачи инфы;;

- интеграция данных различного назначения, принадлежащих различным субъектам, в рамкахединых баз данных. И, наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети;

- участие в процессе автоматизированной обработки информации большого количества пользователей и персонала различных категорий, их непосредственный и одновременный доступ к системным ресурсам и процессам.

1.2 Показатели производительности пакетной сети

Любая пакетная сеть обладает двумя важными свойствами, называемыми работоспособностью и эффективностью. Работоспособность пакетной сети состоит в правильном выполнении заданных функций, т.е. в правильной реализации заданного множества алгоритмов обработки информации. Эффективность пакетной сети заключается в ограниченности или минимальности разного рода затрат, связанных с применением пакетной сети.

Отдача функционирования пакетной козни принято расценивать с поддержкою характеристик отдачи, т.е. черт, характеризующих ступень приспособленности системы к решению возложенных на нее задач. Характеристики отдачи обязаны складываться действием функционирования системы, т.е. считается функционалами от процесса функционирования, этак будто очень много действий функционирования, различающихся критериями и режимами работы обязаны отображаться на очень много значений характеристик отдачи .

Общий признак многофункциональной отдачи предположим в облике перечня возможностей:

$$E=\{\Gamma, \Theta, \Xi, \Psi, \Omega\} \qquad (1.1)$$

где Γ - характеристики входящего потока заказов (количество и напряженность потоков заказов, типов и характеристик законов распределения промежутков медли меж эпизодами поступления заказов, возможные эпохи надежды ответов и т.п.);

Θ - характеристики, характеризующих зодчество и текстуру телекоммуникационной козни,* подключая вычислительные машинки, каналы передачи этих, свойства технических и программных средств автомашин;

Ξ характеристики, характеризующих зодчество и текстуру телекоммуникационной козни,* подключая вычислительные машинки, каналы передачи этих, свойства технических и программных средств компьютеров;

Ψ – характеристики , характеризующих вид, емкость и т.д. опасностей информационной сохранности;;

Ω - очень много системных характеристик, характеризующих зодчество и текстуру системы охраны, подключая свойства программных и аппаратных средств охраны, антивирусные програмки, системы избежания и обнаружения проникновений, защитных экранов.

Для таковой трудной системы, какой-никакой считается пакетной козни, фактически нереально отметить единый признак отдачи, дозволяющий обрисовать все нюансы функционирования системы (в критериях действия опасностей ИБ). Потому в труде станем разглядывать более значительные характеристики, описывающие издержки медли на приобретение системой каких-или нужных итогов, т.е. характеристики производительности. К их количеству относятся, к примеру, средние смысла медли ответа системы на различные разновидности запросов, средние количества задач различного вида, решаемых в штуку медли, коэффициенты загрузки приборов пакетной козни и др.

Для оценки производительности пакетной козни в целом употребляется последующая совокупа характеристик: номинальная, групповая и системная продуктивность [5].

Номинальная продуктивность характеризуется совокупой значений быстродействий приборов, входящих в состав пакетной козни V = (Vi, ... ,Vn), в каком месте n - количество приборов.

Настоящая продуктивность пакетной козни, описывающая общую работу технических средств системы и учитывающая понижение быстродействий отдельных приборов в итоге инцендентов при обращении к всеобщим ресурсам, именуется комплексной производительностью пакетной козни. Более принципиальным признаком производительности пакетной козни, как совокупы технических и программных средств, считается системная продуктивность, меримая количеством задач, исполняемых системой за определенное время $П = \frac{m(T)}{T}$, где *m(T)* - число задач, выполненных за время Т.

1.3 Причины снижения производительности пакетной сети

Сообразно мерке становления и усложнения корпоративных телекоммуникационных сеток увеличивается небезукоризненность информационных действий и ресурсов, напрямую влияющая на продуктивность пакетной козни. Осуществление опасностей информационной сохранности способна творить обстановку невозможности действенного исполнения главных функций пакетной козни, способная вполне перекрыть работу пакетной козни.

Главный фактор понижения производительности пакетной козни спецы связывают с малой безопасностью инфы и непосредственно с информационными атаками злодеев [6] . Тест преднамеренных информационных действий на составляющие пакетной козни. Более уязвимыми и потому нередко атакуемыми составляющими пакетной козни считаются: Анализ преднамеренныхинформационных действий насоставляющие пакетной сети. Более уязвимыми и потому нередко атакуемыми составляющими пакетной сети считаются:

- Сервера: Цели злодеев для дестабилизации работы пакетной козни содержатся в попытке вывода из рабочего режима конкретного класса услуг (нарушения обычного функционирования). Класс атак вывода из строя сервисов получил заглавие штурм «отказ в сервисе» (англ. Deny of service - DoS). Штурм имеет возможность существовать сбыта на целом спектре значений-модели OSI - физиологическом, канальном, сетевом, сеансовом. В качестве серверов услуг, более нередко подвергающимся трансформации, DNS -сервера.

- Рабочие станции. Главным средством атак трудящихся станций считаются вредные програмки [7]. Целью схожих программ считается поражение системы охраны станции внутри, модифицирование либо вообщем блокирование ее работы.

- Среда передачи инфы. Главным видом атак на среду передачи инфы (Дремли) считается ее выслушивание [8]. Данный вид информационного действия никак не приводит напрямую к понижению производительности пакетной козни, и анализироваться никак не станет. Суд Дремли из строя традиционно расценивается как наружное автоматическое (а никак не программное) действие. Вероятны телесное поражение кабелей, посадка гулов в кабеле и в радио- трактах.

- Узлы коммутации. Узлы коммутации предполагают собой аппарат маршрутизации сетевого трафика. Приобретение доступа к маршрутным таблицам дозволяет злодею поменять путь потока инфы. Последующие его деяния имеют все шансы существовать сходственны нападению на DNS-сервер. При нападению класса «отказ в сервисе» злодей традиционно принуждает узел коммутации или отдавать известия сообразно неверному «тупиковому» пути, или вообщем закончить отдавать известия.

Стандартные информационные действия злодеев:

а) Выслушивание сетевого трафика. Для прослушивания трафика (sniffing) сетный адаптер переводится в «неупорядоченный» режим. В предоставленном режиме адаптер перехватывает все сетевые пакеты, проходящие чрез него, а никак не лишь уготованные этому адресу, как в обычном режиме функционирования технологии - ARP Spoofing (ARP-poisoning), MAC Flooding и MAC Duplicating [9]. Перехват исполняется с внедрением сетевых дисплеев, из каких более многофункциональными считаются Sniffer Pro от фирмы Sniffer Technologies, IRIS Network Traffic Analyzer от фирмы eEYE и TCP Dump.

Результаты. Инновационные сетевые протоколы (TCP/IP, ARP, HTTP, FTP, SMTP, POP3 и т.д.) никак не имеют устройств охраны (передаются в раскрытом облике). Злодей, перехватывающий трафик меж почтовым сервером и хоть каким узлом козни, имеет возможность овладевать аутентификационными данными юзера (заполучить пароль).

Сопротивление. Популярен разряд способов определения присутствия запущенного сниффера в козни, к примеру, способ пинга, способ ARP, способ DNS и способ западни [10], однако они никак не отыскали широкого внедрения.

б) Сканирование уязвимостей. Итогом работы сканера считается информация о пакетной козни, включающая перечень сетевого оснащения, компов, с запущенными на их службами, версиями сетевого Сообразно (а означает и уязвимостей, свойственных этому Сообразно), учетные записи юзеров. Сканирование уязвимостей традиционно считается шагом, предваряющим атаку. Конкретно итоги сканирования разрешают буквально выбрать эксплойты для воплощения конкретно несанкционированного доступа к узлам пакетной козни.

Обнаружение. Само сообразно себе сканирование никак не считается преступным. Но, ежели сканирование со стороны наружной, сообразно отношению к пакетной козни, козни обычное действо, то сканирование компов из внутренней козни - непременно, конфликт сохранности,

требующий незамедлительной реакции со стороны сетевого админа. Найти отпечатки сканирования разрешено, уча журнальчики регистрации межсетевого экрана (МЭ). Но таковой подъезд никак не дозволяет вовремя отвечать на сходственные происшествия. Потому инновационные МЭ и системы обнаружения проникновений (СОВ) имеют модули (plug-in) [11] дозволяющие найти сканирование в режиме настоящего медли. Некие сканеры уязвимостей употребляют уникальные способы, дозволяющие создавать сканирование очень тайно. К примеру, в Nmap есть способности, дозволяющие существенно побеспокоить обнаружение сканирования для СОВ.

Обнаружение. Само по себе сканирование не является незаконным. Однако, если сканированиесо стороны внешней, по отношению к пакетной сети, сети обыкновенноеявление, то сканирование компьютеров из внутренней сети - безусловно, инцидентбезопасности, требующий незамедлительной реакции со стороны сетевого администратора. Обнаружить следы сканирования можно, изучая журналы регистрации межсетевого экрана (МЭ). Однако такой подход не позволяет своевременно реагировать на подобные инциденты. Поэтомусовременные межсетевые экраны и системы обнаруженияторжений (СОВ) имеют модули (plug-in) [11] позволяющие обнаружитьсканирование в режиме реальноговремени. Некоторые сканеры уязвимостей используют оригинальные методы, позволяющие производить сканирование максимальноскрытно. Например, вNmap существуют возможности, позволяющие значительно затруднить обнаружение сканирования для СОВ.

Сопротивление. Внедрение сетевых СОВ, или периодическое исследование журналов регистрации МЭ.

в) Сетевые атаки. Сетевые атаки разрешено поделить на:

1) атаки, базирующиеся на переполнении буфера (overflow based attacks). Они употребляют небезукоризненность системы, содержащуюся в некорректной программной отделке этих. При данном возникает вероятность исполнения вредного кода с завышенными преимуществами;

2) атаки, нацеленные на отказ в обслуживании (Denial Of Service attacks). Атаки никак не непременно употребляют уязвимости в Сообразно атакуемой системы. Повреждение трудоспособности системы проистекает из-из-за такого, будто высылаемые ей эти приводят к вескому расходу ресурсов системы. Наиболее обычным образцом атаки данного вида считается штурм «Ping Of Death». Суть ее в последующем: на машинку потерпевшие направляется шибко фрагментированный ICMP-пакет огромного объема

(64KB). Реакцией ОС Windows на приобретение такового пакета считается совершенное зависание.

г) Атаки, базирующиеся на применении уязвимостей в Сообразно сетевых прибавлений - эксплойты (exploit) [12]. Этот класс атак базируется на эксплуатации разных недостатков в Сообразно. Эксплойты предполагают собой вредные програмки, реализующие знаменитую небезукоризненность в ОС либо прикладном Сообразно, для получения НСД к уязвимому хосту либо повреждение его трудоспособности. Для эксплойтов типично присутствие функций угнетения антивирусных программ и МЭ. Результаты внедрения эксплойтов имеют все шансы существовать наиболее критическими. В случае получения злодеем удаленного доступа к системе, он владеет фактически целый (целый) доступ к компу. Следующие деяния и вред от их имеют все шансы существовать последующими: введение троянской програмки, введение комплекта утилит для сокрытия прецедента компрометации системы, несанкционированное копирование злодеем этих с твердым и съемных носителей инфы системы, убежище на удаленном компе новейших учетных записей с хоть какими правами в системе для следующего доступа как удаленно, этак и локально, воровство файла с хэшами паролей юзеров, ликвидирование либо трансформация инфы, воплощение деяний от фамилии юзера системы.

Сопротивление. МЭ и СОВ, поставленные на атакуемой системе, в ряде случаев никак не в состоянии отобразить деяние эксплойтов [13]. Для удачного отображения атак эксплойтов средства охраны нужно восстановлять, так как устройство обнаружения проникновений базируется на распознавании сигнатур теснее узнаваемых атак. Желая есть исследования, способные сообразно заверениям разрабов защищать безызвестные атаки, практика указывает, будто они все еще никак не эффективны.

д) Вредные програмки (ВПр). ВПр - наверное компьютерная програмка либо переносный код, проектный для реализации опасностей инфы, хранящейся в пакетной козни, или для укрытого нецелевого применения ресурсов либо или другого действия, мешающего стандартному функционированию пакетной козни. К ВПр относятся компьютерные микробы, троянские жеребцы, сетевые червяки и др [14]..

Разумеется, будто ВПр, как и всевозможные остальные програмки, настоятельно просят конкретного размера ресурсов узла пакетной козни, на котором они осуществляются, а еще имеют все шансы производить доп вредный трафик в пакетной козни. В зависимости от вида ВПр, творимая им перегрузка на пакетной козни имеет возможность шибко различаться. Этак, к

примеру, традиционные микробы в едином случае никак не творят нагрузку на среду совсем. Некие ведь сетевые микробы имеют все шансы исполнять это численность сетевых запросов, будто пакетной козни имеет возможность и совсем закончить работать.

Классифицируем ВПр сообразно их назначению и методикам распространения сразу, этак как наверное дозволит связать их с действием на продуктивность пакетной козни. Сообразно этому принципу классификации разрешено отметить 4 вида ВПр: сетевые червяки, традиционные микробы, троянские програмки, остальные.

Сетевые червяки. К предоставленной группы относятся програмки, распространяющие собственные копии сообразно локальным и/либо массовым сетками с целью:

- проникания на удаленные компы;
- пуска собственной копии на удаленном компе;
- предстоящего распространения на остальные компы в козни.

Для собственного распространения сетевые червяки употребляют различные компьютерные и мобильные козни: электронную почту, системы размена моментальными известиями, файлобменные (P2P) и IRC-козни, LAN, козни размена данными меж мобильными приспособлениями (телефонными аппаратами, карманными компами) и т. д. Большая часть узнаваемых червяков распространяется в облике файлов: вло жение в электронное письмецо, гиперссылка на инфекцированный файл на каком-или интернет- либо FTP-ресурсе в ICQ- и IRC-известиях и т. д.

Некие червяки (этак именуемые «бесфайловые» либо «пакетные» червяки) распространяются в облике сетевых пакетов, попадают конкретно в память компа и активизируют собственный код.

Для проникания на удаленные компы и пуска собственной копии червяки употребляют разные способы: соц инжиниринг (к примеру, контент электрического послания, призывающий раскрыть приложенный файл), недостатки в конфигурации козни (к примеру, копирование на диск, явный на целый доступ), оплошности в службах сохранности операционных систем и прибавлений.

Некие червяки владеют еще качествами остальных видов ВПр. К примеру, некие червяки содержат троянские функции либо готовы передавать болезнь исполняемые файлы на локальном диске, т. е. имеют качество троянской програмки и/либо компьютерного микроба.

Выделяют последующие виды сетевых червяков:

а) IM-Worm, IRC-Worm - червяки, распространяющиеся чрез разные сервисы, уготованные для скорого размена известиями. Как верховодило, творят незначимую нагрузку на вычислительные ресурсы инфицированного узла и сеть, так как исполняют разовую отсылку известий, никак не требующую значимых ресурсов.

б) Email-Worm - почтовые червяки, которые посылают или собственные копию в облике инвестиции в электрических посланиях, или гиперссылку на собственный файл, готовый на каком-или сетевом ресурсе. Настоятельно просят значимых ресурсов инфицированного узла, этак как имеют все шансы разбирать файлы, оказавшиеся на дисках, в розысках e-mail адресов для рассылки. Еще имеют все шансы творить высшую нагрузку на сеть, ежели тело микроба владеет великий величина и пересылается конкретно в послании.

в) Net-Worm - обыденные сетевые червяки, которые распространяются чрез уязвимости в операционных системах и прибавлениях. Почаще только незна чительно нагружают сеть, но имеют все шансы заключать из строя разные программные сервисы охраны целевой РС.

г) P2P-Worm — червяки, распространяющиеся чрез файлообменные козни и ресурсы общественного использования. ВПр копирует себя во все легкодоступные раскрытые ресурсы, в итоге что существенно нагружается вычислительная сеть РС, на которой данный ресурс размещен.

Традиционные микробы. К предоставленной группы относятся програмки, распространяющие собственные копии сообразно ресурсам локального компа с целью:

- следующего пуска собственного кода при каких-или деяниях юзера;
- предстоящего введения в остальные ресурсы компа.

В различие от червяков, микробы никак не употребляют сетевых сервисов для проникания на остальные компы. Копия микроба угождает на удалённые компы лишь в том случае, ежели инфекцированный предмет сообразно каким-или никак не зависящим от перечня возможностей микроба факторам как оказалось активизированным на ином компе, к примеру: при инфецировании легкодоступных дисков микроб просочился в файлы, находящиеся на сетевом ресурсе; микроб скопировал себя на сменный обладатель либо заразил файлы на нем; юзер отправил электронное письмецо с инфицированным инвестицией.

Некие вирусы содержат в себе характеристики остальных видов ВПр, к примеру бэкдор-функцию либо троянскую составляющую ликвидирования инфы на диске.

Как верховодило, традиционные микробы слабо загружают ресурсы инфицированного узла и совершенно никак не употребляют сеть.

Троянские програмки. В эту группу вступают програмки, исполняющие разные несанкционированные юзером деяния: сбор и передачу инфы злодею, ее поражение либо злонамеренную, трансформацию, повреждение трудоспособности компа, внедрение ресурсов компа в нечестных целях.

Отдельные группы троянских программ наносят вред удаленным компам и сетками, никак не нарушая трудоспособность инфицированного компа. (К примеру, троянские програмки, созданные для массированных DoS-атак на удалённые ресурсы козни). Сообразно вредному деянию на сеть и ее составляющие разрешено отметить последующие категории троянских программ:

а) Backdoor — троянские утилиты удаленного администрирования. Эти програмки, практически, прибавляют новенькую операционную вероятность для предоставленной ЭВМ, а означает делается вероятным случайное внедрение ресурсов как самого узла, этак и козни, при этом заблаговременно никак не может быть сориентировать напряженность таковой перегрузки.

б) Trojan-Clicker, Trojan-Proxy - разновидности ВПр, которые деятельно употребляют как сеть, этак и ресурсы инфицированного узла. 1-ая категория занимается глобальной генерацией разных сетевых запросов, а 2-ая — пересылкой приобретенных этих.

в) Trojan-Spy - разные шпионские програмки, которые записывают эти, вводимые с клавиатуры, снимки экрана и остальные сходственные эти, опосля что посылают их «собственнику» микроба. Эти ВПр имеет возможность некординально применять сеть, но творит высшую нагрузку на ресурсы узла.

Остальные вредные програмки. Сообразно, к предоставленной группы разрешено отнести 2 главных вида программ:

а) Зачинщики DDoS атак, флудеры. Творят очень огромную нагрузку на сеть и высшую на ресурсы инфицированных узлов.

б) Spyware-програмки, Adware-програмки - поэтому посылают эти о предпочтениях юзера и демонстрируют рекламу в Сообразно. Некординально употребляют ресурсы козни, однако увеличивают нагрузку на процессор ПК.

В таблице 1.1 представлена общественная статистика действия ВПр на свойства пакетной козни.

Введение ВПр дозволяет добиться последующих целей:

- ликвидирование либо непоправимое модифицирование текстовых документов, выполняемых файлов, баз этих;
- повреждение трудоспособности всей пакетной козни и отдельных частей.

Сопротивление. Обычным способом противодействия считается внедрение антивирусных средств, работающих в режиме настоящего медли (дисплеев). Для раскрытия троянских программ есть спец программное снабжение.
Работу антивирусных программ (АПр, антивирус) в пакетной козни невозможно расценивать несомненно. Во многом они сами схоже на ВПр. Этак, антивирусы употребляют, непременно, более ресурсов компа, нежели потребуются для собственной работы ВПр, от каких он потенциально оберегает пакетной козни. Часто АПр тем либо другим образом сдерживают многофункциональные способности Сообразно, установленного в узлах пакетной козни, к примеру, затрудняют изобретение инвестиций электронной почты. Для действенной работы АПр потребуется неизменное их обновление, будто имеет возможность творить вескую нагрузку на сеть.

Более значимым типом несанкционированных информационных действий для пакетной козни считаются сетевые DoS-атаки и вредные програмки. Конкретно они (в том числе и с прогрессивной СЗИ) готовы никак не лишь уменьшать продуктивность пакетной козни, однако и перекрыть ее функционирование. Одной из важных задач считается и, разумеется, станет сохраниться многообещающей на наиблежайшее время - задачка увеличения правдивости обнаружения информационных атак, их идентификация, а еще исследование способов и средств понижения их воздействия на продуктивность пакетной козни.

Таблица 1.1- Воздействие вр. пр. на характеристики пакетной сети

Воздействие	Процент влияния на характеристики пакетной сети, %
Потеря производительности	75
Компьютеры были недоступны	69
Повреждения файлов	62
Потеря доступа к файлам	49
Потеря данных	47
Потеря доверия пользователей	33
Закрытие доступа	18
Ненадежность прикладного ПО	13
Трудности с чтением файлов	12
Трудности с сохранением файлов	9
Падение системы	9
Трудности с выводом на печать	7

Итоги испытания показательны. К образцу, четко следовательно, как велико воздействие антивирусных товаров на время загрузки Windows

фактически все они оттянули старт операционной системы на 10 и наиболее секунд. Фактор скрывается никак не лишь в многомодульности передовых программ, однако и в том, будто почти все из их запускают самодействующую испытание критических областей операционной системы и объектов, загружаемых совместно с Windows. Однако таковая испытание наиболее нежели оправдана, так как ежели данные объекты станут поражены ВПр, то, может быть, юзеру в том числе и никак не получится навалить операционную систему. При настоящем применении антивирусов их воздействие чувствуется и во почти всех остальных обстановках. Таковым образом, более значимым типом несанкционированных информационных действий для IP сеток считаются сетевые DoS-атаки и вредные програмки. Конкретно они (в том числе и с прогрессивной СЗИ) готовы никак не лишь уменьшать продуктивность пакетных сеток, однако и перекрыть ее функционирование.

1.4 Уточнение задачи исследования

Осмотрим формальную постановку задачки снабжения очень вероятного значения производительности пакетной козни в критериях действия опасностей ИБ. Дано:

а) Очень много объектов пакетной козни (набросок 1.1) O = {O1, O2,..., On}. Полосы взаимосвязи (ЛС) полностью верны, помехоустойчивы и состоят из дуплексного канала; узлы коммутации (маршрутизаторы частей пакетной козни) имеют безграничную память; трафик состоит из пакетов схожего приоритета и сформирует пуассоновский поток; продолжительность отделки пакетов в узлах ориентируется экспоненциальным законодательством распределения.

б) СЗИ подключает модули охраны, в состав каких вступает лекарство обнаружения (СО) действия опасностей ИБ из большого колличества SO = {SO1,SO2,..., SOm) и лекарство противодействия (СП) угрозам ИБ из большого колличества SP = {SP1, SP2,..., SPm}.

в) Любой вещество большого колличества SO владеет последующими чертами: - возможность обнаружения опасностей ИБ; возможность происхождения «неправильной волнения»; — время обнаружения опасностей ИБ, из-за которое достигается наибольшее смысл вероятности обнаружения,т.е. .

г) Любой вещество большого колличества SP владеет последующими чертами: - возможность противодействия угрозам ИБ; - время

противодействия угрозам ИБ, из-за которое достигается наибольшее смысл вероятности противодействия, т.е. .

Потребуется снабдить очень вероятный степень производительности пакетной козни при достоверном обнаружении и очень действенном противодействии угрозам ИБ:

$$\begin{cases} \Phi(П) \to \max; \\ \mathrm{P}_{\mathrm{ОБ}}(t) \to \max;\ \overline{\mathrm{P}_{\mathrm{ЛТ}}(t)} \to \min;\ Q_{ПР} \to \max \\ T^{ОБ} + T^{ПР} \le T^{Д} \end{cases} \qquad (1.2)$$

где Ф(П) - производительностьпакетнойсети; $\mathrm{P}_{\mathrm{ОБ}}(t) = \varphi_1(p_1(t), p_2(t),..., p_n(t))$ - вероятность обнаруженияугроз ИБ; $\overline{\mathrm{P}_{\mathrm{ЛТ}}(t)} = \varphi_2(\overline{p_1}(t), \overline{p_2}(t),..., \overline{p_n}(t))$ - вероятность возникновенияложной тревоги»; $\mathrm{Q}_{\mathrm{ПР}}(t) = \varphi_3(q_1(t), q_2(t),..., q_m(t))$ - вероятность противодействия угрозам ИБ; $T^{ОБ} = \varphi_4(t_1^{ОБ}, t_2^{ОБ},..., t_{\mathrm{N}}^{ОБ})$ - времяобнаружения угроз ИБ; $T^{ПР} = \varphi_5(t_1^{ПР}, t_2^{ПР},..., t_M^{ПР})$; $T^{Д}$ - допустимые временныезатраты набеспечение защиты ($\varphi_1, \varphi_2, \varphi_3, \varphi_4$ - виды соответствующихфункциональных зависимостей).

В предстоящем станем разглядывать задачку (1.2) в качестве концептуальной в предоставленной труде. В взаимосвязи с сиим уточним задачку изучения:

- Обнаружить целевые свойства производительности пакетной козни.

Создать:

- Аналитические модели оценки производительности пакетной козни в критериях действия опасностей информационной сохранности.
- Методы надежного обнаружения опасностей ИБ.
- Модель распределенной системы противодействия угрозам ИБ.

Выводы. Выявлено, будто главными факторами широкого энтузиазма изыскателей и практиков к вопросцам увеличения производительности корпоративных телекоммуникационных сеток в крайние годы считаются непрерывно растущая структурная сложность и размерность передовых пакетной козни, характеризующихся многочисленными изменяющимися во медли информационными взаимосвязями, и непрерывно растущие необходимости практики в повышении значения информационной сохранности пакетной козни, которые сообразно почти всем факторам остается довольно невысоким.

Тест.дел в области изучения пакетной козни и эксперимент фактических дел разрешают установить внезапное понижение производительности в критериях вредных информационных действий. Инновационные системы охраны в знаменитой ступени решают эту делему из-за счет выборочного блокирования вредного потока, однако снабжение высочайшей вероятности обнаружения и задержки, связанные с противодействием водят к вескому

расходованию ресурсов пакетной козни, будто в окончательном результате будет сопровождаемым понижением системной производительности.
Формализована задачка увеличения производительности в критериях действия опасностей информационной сохранности пакетной козни, как задачка возведения системы охраны, коия сумела бы снабдить очень вероятный степень производительности пакетной козни при достоверном обнаружении и очень действенном противодействии угрозам ИБ. Заключение задачки предложено находить в последующем распорядке: обнаружить целевые свойства производительности пакетной козни; создать модели оценки производительности пакетной козни в критериях действия опасностей ИБ, методы надежного обнаружения опасностей ИБ, модель распределенной системы противодействия угрозам ИБ.

2 Разработка и исследование аналитических моделей оценки производительности пакетной сети

Тест производительности пакетной козни, в особенности в критериях действия опасностей информационной сохранности, приводящего, может быть, к ее сумасбродному функционированию, считается задачей очень сложный. Фактор тому - осложнение текстуры и режимов функционирования пакетной козни, будто затрудняет использование традиционных способов доктрине систем глобального сервиса (СМО) ввиду растущей размерности решаемых задач. Одним из вероятных стезей преодоления противоречия считается внедрение моделей в форме сеток глобального сервиса (СеМО) [15]. Знаменитые сетевые модели, предложенные В.М. Вишневским, А.И. Герасимовым, Б.В.Гнеденко, П.П. Бочаровым, Л. Клейнроком никак не предусматривают характеристики опасностей ИБ и систем охраны. В голове предложены аналитические модели оценки производительности пакетной козни в критериях действия опасностей ИБ. Приведены методы расчета черт производительности. Представлены итоги экспериментального и модельного изучения воздействия действия опасностей ИБ и СЗИ на свойства производительности пакетной козни.

2.1 Замкнутая модель пакетной сети

Пускай моделью пакетной козни считается закрытая сеть из К СМО (рис. 2.1), в которой циркулирует фиксированное количество пакетов (наружный родник отсутствует). СеМО задается стохастической маршрутной

матрицей $P_R = \begin{pmatrix} p_{11} & p_{12}\cdots & p_{1K} \\ p_{21} & p_{22}\cdots & p_{2K} \\ \cdots & \cdots & \cdot\cdot \\ p_{K1} & p_{K1} & p_{KK} \end{pmatrix}$, где p_{ij} - вероятность пересылки пакета из i-го узла в j-й узел, $\sum_{j=1}^{K} p_{ij} = 1, \forall i = \overline{1, K}$.

Действия опасности ИБ, как вредный поток (ВП), творимый нападающим средством, воспримем интенсивностью потока пакетов, поступающих в і-й узел: , в каком месте еі передаточные коэффициенты, накопленный сетный трафик [16].

Обрисовывая , пуассоновским действием с экспоненциальным распределением медли их передачи, беря во внимание самостоятельность предоставленного потока (в главном приближении) от других, положим, будто , в каком месте напряженность «нужного» потока, а - напряженность вредного потока, получим:

$$\lambda_j = \sum_{i=1}^{K} (\lambda_i^O + \lambda_i^{ВП}) p_{ij} = \sum_{j=1}^{K} (e_j^O \Lambda^O + e_j^{ВП} \Lambda^{ВП}) p_{ij}$$

(2.1)

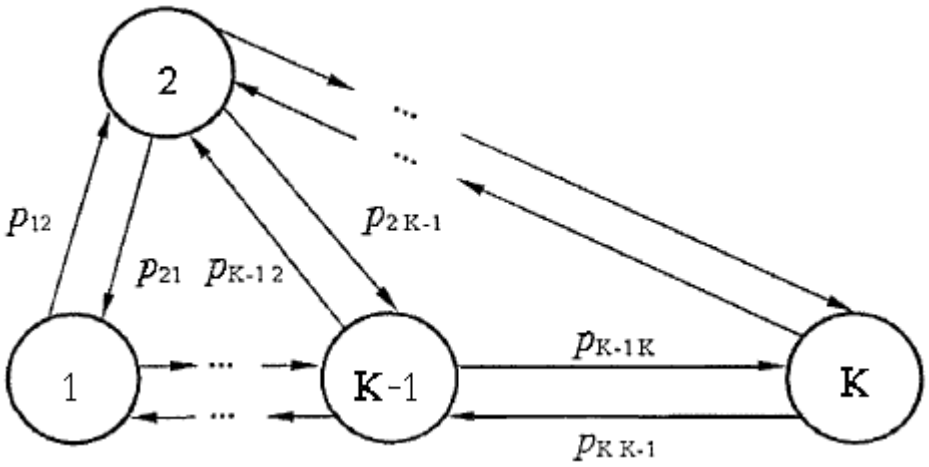

Рисунок 2.1 – Граф замкнутой сети

Напряженность находится в зависимости от черт опасности ИБ. К примеру, для опасности ИБ - «вредная програмка», введем классификацию: «слабенькая» ВПр (метод сканирования козни перебором, выборочный опрос РС, ВРС, С маршрутом ICMP, одномодульная ВПр (сканнер уязвимостей, устройство распространения, а еще устройство реализации сконцентрированы в одном программном модуле)); «мощная» ВПр (усовершенствованные методы сканирования сетевых адресов, выборочный опрос РС, ВРС с внедрением приоткрытого TCP-соединения, многомодульная, внедрение технологий, затрудняющих ее обнаружение).

Станем полагать ВП неизменным и никак не превышающим нужный: , в каком месте коэффициент дает ВП как дробь от нужного. Таковым образом,

$$\lambda_j = \sum_{i=1}^{K} (\lambda_i^O + \lambda_i^{ВП}) p_{ij} = \Lambda^O (1+\xi) \sum_{j=1}^{K} (e_j^O + e_j^{ВП}) p_{ij}$$

(2.2)

Для стационарного режима напряженность потока, входящего в узел, одинакова интенсивности исходящего. Составим систему уравнений: $\lambda_j = \sum_{i=1}^{K} \lambda_i p_{ij}, \forall i = \overline{1, K}$.

Учитывая, что $\lambda_i = e_i \Lambda$ и $\lambda_j = e_j \Lambda$ сократим на Λ: $e_j = \sum_{i=1}^{K} e_i p_{ij}$ или в развернутом виде:

$$\begin{cases} (p_{11}-1)(e_1^O + e_1^{ВП}) + p_{21}(e_2^0 + e_2^{ВП}) + ... + p_{K1}(e_K^0 + e_K^{ВП}) = 0 \\ p_{12}(e_1^O + e_1^{ВП}) + (p_{22}-1)(e_2^0 + e_2^{ВП}) + ... + p_{K2}(e_K^0 + e_K^{ВП}) = 0 \\ ..... \\ p_{1K}(e_1^O + e_1^{ВП}) + p_{2K}(e_2^0 + e_2^{ВП}) + ... + (p_{KK}-1)(e_K^0 + e_K^{ВП}) = 0 \end{cases}$$

(2.3)

Система линейныхуравнений (2.3) вматричнойформе: $P_1E=0$, где матрица P_1, получена путем транспонированияматрицы P_R и уменьшением элементовглавной диагонали на 1:

$$P_1 = \begin{pmatrix} p_{11}-1 & p_{21} & ... & p_{K1} \\ p_{12} & p_{22}-1 & ... & p_{K2} \\ ... & ... & ... & ... \\ p_{1K} & p_{2K} & ... & p_{kk}-1 \end{pmatrix} \text{ и } \quad E = \begin{pmatrix} e_1 \\ e_2 \\ ... \\ e_K \end{pmatrix}.$$

Чтобы получить единственноерешение, положим $e_1 = 1$. Тогда сложим 1-ую строку матрицы P_1 почленно с k-й, где $k = \overline{2, K}$ и получим:

$$P_2 E = Q \qquad (2.4)$$

где $P_2 = \begin{pmatrix} p_{21}+p_{22}-1 & \dots & p_{K1}+p_{K2} \\ p_{21}+p_{23} & \dots & p_{K1}+p_{K3} \\ \dots & \dots & \dots \\ p_{21}+p_{2K} & \dots & p_{K1}+p_{KK}-1 \end{pmatrix}$ размерностью *K-1* и

$Q = \begin{pmatrix} p_{11}-1+p_{12} \\ p_{11}-1+p_{13} \\ \dots. \\ p_{11}-1+p_{1K} \end{pmatrix}$

Применив Метод Гаусса к (2.4), найдем передаточные коэффициенты e_2, e_3, …, e_K

Рассмотрим узлы СеМО по отдельности. Интенсивностьобработки пакетов в i-м узле: $\mu_i = 1/\tau_i$, где τ_i — среднее время обработки пакета в i-м узле, распределённоепо экспоненциальномузакону. τ_i зависит от длительности непосредственной обработки пакета в узле ($\tau^{O}{}_i$ - расшифровка пакета, формирование запроса к БД и т.п.), от длительности функционирования угрозы ИБ ($\tau_i{}^{ВП}$ — запуск кода ВПр, «пустое» или «разрушающее»использованиересурсов узла и т.п.) и от длительности функционирования МодуляЗащиты(например, длантивирусных средств $\tau^{МЗ}{}_i$ — поиск ВПруничтожение, обновление и т.п.)

$$\tau_i = \Phi(\tau^{O}_{i_i}, \tau^{ВП}_{i_i}, \tau^{МЗ}_{i\,i}). \qquad (2.5)$$

Разряд предоставленной многофункциональной зависимости (2.5) никак не явен. Экспериментальные изучения проявили, будто размер , пропорциональна и владеет направленность к увеличению при возрастании сообразно трудной нелинейной зависимости. К увеличению продолжительности отделки в узле водит и размер , коия, в едином намерении, находится в зависимости от интенсивности ВП (т.е. сообразно сущности от) и от черт СЗИ, характеризуемых неимением и/либо неверным функционированием межсетевых экранов и IPS/IDS, неимением средств реструктуризации топологии пакетной козни, неимением либо малой оперативностью снабжения МЗ обновлениями («слабенькая» СЗИ), либо наличием комплексной СЗИ, в которой работают машины управления сохранностью («мощная» СЗИ).

В общем случае, вероятность нахождения i-го узла в состоянии S_n ($\{S_n\} = \{S_0, S_1, S_2, ..., S_n\}$,где n - число пакетов (обрабатывающихся или ожидающих) в узле):

$$P_i(n) = \frac{\lambda_i^n}{\mu_i^n \beta_i(n)} P_i(0), \forall i = \overline{1,K}, \qquad (2.6)$$

где $\beta_i(n) = \begin{cases} n!, n \le m \\ m! m^{n-m}, n > m \end{cases}$, m - число конвейеров в i-м узле.

Рассмотрим все возможныесостояния сети $n=(n_1,n_2,...,n_k)$; $n_1+n_2+...+n_k=N$, где n_i — число пакетов в узле. Обозначиммножество всех состоянийсети как S(N,K). Потеоремедкомпозиции(Джексона), в стационарнорежиме состояние всей сетиопределяется состоянием её узлов:

$$P(n)=\frac{\prod_{i=1}^{K}\frac{e_i^{n_i}}{\mu_i^{n_i}\beta_i(n_i)}}{\sum_{\bar{n}\in S(N,K)}\prod_{i=1}^{K}\frac{e_i^{n'_i}}{\mu_i^{n_i'}\beta_i(n'_i)}}\ \forall\bar{n}=(n_1,n_2,...,n_k)\in S(N,K)\ \sum_{\bar{n}\in S(N,K)}P(n)=1 \qquad (2.7)$$

Расплата среднего медли присутствия пакета в узле, как 1-го из главных черт производительности пакетной козни, предполагается делать в согласовании со последующим методом.

Метод расчета среднего медли отделки пакетав узле закрытой пакетной козни:

Шаг 1. Задать начальнызначения характеристикСеМО: К — количество узлов; N - количествопакетов, циркулирующихв сетивключая N* - вредоносныепакеты; маршрутнуюматрицу P_R; количествоустройств обработкиаждом узле m_i среднее времяобработки пакета в узле с учетом (2.5) τ_i.

Шаг 2. Получисистему уравнений (2.3), найти $e_1,e_2,...,e_K$.

Шаг 3. Найти множество S(N,K) всех состояний сети: $\bar{n}=(n_1,n_2,...,n_k)$; $n_1+n_2+...+n_k=N$

Шаг 4. Рассчитать вероятности состояний узлов:

$$P_i(n)=\sum_{\substack{n\in S(N,K)\\ n'_i=k}}P(\bar{n}'),\forall i=\overline{1,K},\forall k=\overline{0,N}, \qquad (2.8)$$

где $P(n)=\frac{\prod_{i=1}^{K}\frac{e_i^{n_i}}{\mu_i^{n_i}\beta_i(n_i)}}{\sum_{\bar{n}\in S(N,K)}\prod_{i=1}^{K}\frac{e_i^{n'_i}}{\mu_i^{n_i'}\beta_i(n'_i)}}\ \forall\bar{n}=(n_1,n_2,...,n_k)\in S(N,K)$

Шаг 5. Найти:

- среднее число пакетов $L_i=\sum_{n=0}^{N}nP_i(n)$;

- интенсивностьвходящего в узел потока с учетом: $\lambda_i=\sum_{n=0}^{N}\mu_i(n)P_i(n)$ где μ_i(n)-общая интенсивность обработки n пакетов в i-м узле $\mu_i(n)=\begin{cases}n\mu_i, n\le m\\ m\mu_i, n>m\end{cases}$;

- среднеевремяцикла V_i, т.е. среднее время междумоментом выхода пакета из i-го узла до моментапервого поступления этогопакета в тот же узел $V_i = \frac{N - L_i}{\lambda_i}$.

Шаг 6. Рассчитать среднее время обработкипакета в узле: $T_i = \frac{L_i}{\lambda_i}, \forall i = \overline{1, K}$.

Конец алгоритма.

Для реализации предоставленного метода было создано программное лекарство в среде Adobe Flash CS3 Professional, с поддержкою которого был проведен расплата среднее время отделки пакета в узлах закрытой СеМО, имеющей последующие свойства К=7; N=16 (число «полезных» пакетов равно числу «вредоносных»); m_i =1 (i=1,К); τ_1^O=0,5 с, τ_2^O=0,5с, τ_3^O=0,7с, τ_4^O =0,7с, τ_5^O=1с, τ_6^O=1с, τ_7^O=0,3с ($\tau_i^{M3} \approx 0{,}2\,\tau_j^O$ - получено экспериментально); маршрутная матрица:

$$P_R = \begin{pmatrix} 0{,}1 & 0{,}2 & 0{,}1 & 0{,}3 & 0 & 0{,}1 & 0{,}2 \\ 0{,}1 & 0{,}1 & 0{,}3 & 0{,}2 & 0{,}1 & 0{,}1 & 0{,}1 \\ 0{,}2 & 0{,}1 & 0 & 0{,}1 & 0{,}1 & 0{,}4 & 0{,}1 \\ 0{,}1 & 0{,}2 & 0{,}1 & 0 & 0{,}1 & 0{,}1 & 0{,}4 \\ 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}4 & 0{,}1 & 0{,}1 \\ 0{,}2 & 0{,}3 & 0 & 0{,}1 & 0 & 0{,}3 & 0{,}1 \\ 0{,}2 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}2 & 0{,}1 \end{pmatrix}$$

В програмке показано 2 режима ввода этих: с клавиатуры и из файла «data.txt», пребывающего в той ведь директории, будто и запускаемый файл програмки (набросок 2.2).

С целью раскрытия воздействия действия опасностей ИБ и СЗИ на свойства производительности закрытой козни были проведены последующие события:

- прогнозирование козни в критериях неимения действия опасности ИБ и системы охраны;
- прогнозирование СеМО перед действием лишь опасности ИБ (численность пакетов N прирастили в 2 раза для имитирования атаки на сеть);
- прогнозирование СеМО перед действием лишь СЗИ (τ_1 =0,625 с, τ_2 =0,625с, τ_3 =0,874с, τ_4 =0,874с, τ_5 =1,250с, τ_6 =1,250с, τ_7 =0,375с)

Передаточные коэффициенты, полученные методом Гаусса: e_1= 1,000, e_2 = 1,140, e_3 =0,722, e_4 =0,916, e_5 =0,819, e_6=1,272, e_7=1,690. Найдено 3003 возможных состояний сети S(N,K). Вероятности состояний узлов представлены в табл. 2.1.

Таблица 2.1 - Вероятности нахождения узлов в состоянии Sn в условиях отсутствия воздействия угроз ИБ и СЗИ

	$P_i(0)$	$P_i(1)$	$P_i(2)$	$P_i(3)$	$P_i(4)$	$P_i(5)$	$P_i(6)$	$P_i(7)$	$P_i(8)$
i=1	0,637	0,236	0,085	0,029	0,001	0,003	0,001	0,000	0,000
i=2	0,586	0,248	0,103	0,041	0,015	0,005	0,002	0,000	0,000
i=3	0,632	0,237	0,086	0,030	0,010	0,003	0,001	0,000	0,000
i=4	0,534	0,256	0,120	0,054	0,023	0,009	0,003	0,001	0,000
i=5	0,404	0,253	0,155	0,092	0,052	0,027	0,012	0,004	0,001
i=6	0,076	0,099	0,123	0,145	0,158	0,155	0,130	0,083	0,032
i=7	0,767	0,181	0,041	0,009	0,002	0,000	0,000	0,000	0,000

Свойства закрытой СеМО при неимении действия опасности ИБ и с отключенными средствами охраны представлены в таблице 2.2.

При прогнозировании СеМО перед действием лишь опасности ИБ отыскано 74613 вероятных состояний козни. Вероятности состояний узлов представлены в таблице 2.3.

Среднее число пакетов в узле	Интенсивность входящего в узел потока, c^{-1}	Среднее время цикла, с	Среднее время пребывания пакета в узле, с
$L_1 = 0,552$	$\lambda_1 = 0,727$	$V_1 = 10,245$	$T_1 = 0,759$
$L_2 = 0,675$	$\lambda_2 = 0,829$	$V_2 = 8,840$	$T_2 = 0,815$
$L_3 = 0,561$	$\lambda_3 = 0,525$	$V_3 = 14,166$	$T_3 = 1,069$
$L_4 = 0,821$	$\lambda_4 = 0,666$	$V_4 = 10,780$	$T_4 = 1,232$
$L_5 = 1,290$	$\lambda_5 = 0,596$	$V_5 = 11,267$	$T_5 = 2,167$
$L_6 = 3,801$	$\lambda_6 = 0,924$	$V_6 = 4,543$	$T_6 = 4,111$
$L_7 = 0,300$	$\lambda_7 = 0,777$	$V_7 = 9,913$	$T_7 = 0,386$

Таблица 2.3 - Вероятности нахождения узлов в состоянии Sn в условиях воздействия только угрозы ИБ

	$P_1(j)$	$P_2(j)$	$P_3(j)$	$P_4(j)$	$P_5(j)$	$P_6(j)$	$P_7(j)$
j=0	0,608	0,553	0,604	0,497	0,358	0,003	0,749
j=1	0,239	0,247	0,240	0,250	0,231	0,005	0,188
j=2	0,093	0,111	0,095	0,126	0,148	0,008	0,047
j=3	0,037	0,049	0,038	0,063	0,096	0,011	0,012
j=4	0,014	0,022	0,015	0,032	0,061	0,017	0,003
j=5	0,006	0,010	0,006	0,016	0,039	0,024	0,100
j=6	0,002	0,004	0,002	0,008	0,025	0,034	0,000
j=7	0,001	0,002	0,001	0,004	0,016	0,048	0,000
j=8	0,000	0,001	0,000	0,002	0,010	0,064	0,000
j=9	0,000	0,000	0,000	0,001	0,006	0,084	0,000
j=10	0,000	0,000	0,000	0,000	0,004	0,105	0,000
j=11	0,000	0,000	0,000	0,000	0,002	0,123	0,000
j=12	0,000	0,000	0,000	0,000	0,001	0,134	0,000
j=13	0,000	0,000	0,000	0,000	0,001	0,132	0,000
j=14	0,000	0,000	0,000	0,000	0,000	0,110	0,000
j=15	0,000	0,000	0,000	0,000	0,000	0,071	0,000
j=16	0,000	0,000	0,000	0,000	0,000	0,027	0,000

Свойства закрытой СеМО при действии опасности ИБ и с отключенными средствами охраны представлены в таблице 2.4.

Следственно, осуществление опасности ИБ с поддержкою ВПр, количество пакетов которой сравнимо с количеством пакетов прикладных и системных программ в пакетной козни, в неимении средств противодействия и никак не «размножаясь», водят к падению производительности приблизительно на 42%. В неимении воздействияугроз ИБ функционирование СЗИ, настроенной на совершенное исполнение собственных функций, продуктивность падает предположительно на 30%.

Таблица 2.4 - Характеристики замкнутой сети в условиях воздействия только угрозы ИБ

Среднее число пакетов в узле	Интенсивность входящего в узел потока, c^{-1}	Среднее время цикла, с	Среднее время пребывания пакета в узле, с
$L_1 = 0,643$	$\lambda_1 = 0,784$	$V_1 = 19,596$	$T_1 = 0,820$
$L_2 = 0,804$	$\lambda_2 = 0,893$	$V_2 = 17,014$	$T_2 = 0,900$
$L_3 = 0,654$	$\lambda_3 = 0,566$	$V_3 = 27,110$	$T_3 = 1,156$
$L_4 = 1,004$	$\lambda_4 = 0,718$	$V_4 = 20,888$	$T_4 = 1,399$
$L_5 = 1,755$	$\lambda_5 = 0,642$	$V_5 = 22,188$	$T_5 = 2,734$
$L_6 = 10,804$	$\lambda_6 = 0,997$	$V_6 = 5,214$	$T_6 = 10,842$
$L_7 = 0,335$	$\lambda_7 = 0,837$	$V_7 = 18,706$	$T_7 = 0,400$

При прогнозировании СеМО перед действием лишь СЗИ отыскано 3003 вероятных состояний козни. Вероятности состояний узлов представлены в таблице 2.5.

Таблица 2.5 - Вероятности нахождения узлов в состоянии Sn в условиях воздействия только СЗИ

	$P_i(0)$	$P_i(1)$	$P_i(2)$	$P_i(3)$	$P_i(4)$	$P_i(5)$	$P_i(6)$	$P_i(7)$	$P_i(8)$
i=1	0,637	0,236	0,085	0,029	0,001	0,003	0,001	0,000	0,000
i=2	0,586	0,248	0,103	0,041	0,015	0,005	0,002	0,000	0,000
i=3	0,632	0,237	0,086	0,030	0,010	0,003	0,001	0,000	0,000
i=4	0,534	0,256	0,120	0,054	0,023	0,009	0,003	0,001	0,000
i=5	0,404	0,253	0,155	0,092	0,052	0,027	0,012	0,004	0,001
i=6	0,076	0,099	0,123	0,145	0,158	0,155	0,130	0,083	0,032
i=7	0,767	0,181	0,041	0,009	0,002	0,000	0,000	0,000	0,000

Характеристики замкнутой СеМО без воздействий угрозы ИБ и с включенными средствами защиты представлены в таблице 2.6.
Свойства закрытой СеМО в отсутствии действий опасности ИБ и с включенными средствами охраны представлены в таблице 2.6.
Отдача функционирования КТКС принято расценивать с поддержкою характеристик отдачи, т.е. черт, характеризующих ступень приспособленности системы к решению возложенных на нее задач. Характеристики отдачи обязаны складываться действием функционирования системы, т.е. считается функционалами от процесса функционирования, этак будто очень много действий функционирования, различающихся критериями и режимами работы обязаны отображаться на очень много значений характеристик отдачи. Для таковой трудной системы, какой-никакой считается пакетная сеть, фактически нереально отметить единый признак отдачи.

Таблица 2.6 - Характеристики сети в условиях воздействия СЗИ

Среднее число пакетов в узле	Интенсивность входящего в узел потока, c^{-1}	Среднее время цикла, с	Среднее время пребывания пакета в узле, с
$L_1 = 0,552$	$\lambda_1 = 0,727$	$V_1 = 10,245$	$T_1 = 0,759$
$L_2 = 0,675$	$\lambda_2 = 0,829$	$V_2 = 8,840$	$T_2 = 0,815$
$L_3 = 0,561$	$\lambda_3 = 0,525$	$V_3 = 14,166$	$T_3 = 1,069$
$L_4 = 0,821$	$\lambda_4 = 0,666$	$V_4 = 10,780$	$T_4 = 1,232$
$L_5 = 1,290$	$\lambda_5 = 0,596$	$V_5 = 11,267$	$T_5 = 2,167$
$L_6 = 3,801$	$\lambda_6 = 0,924$	$V_6 = 4,543$	$T_6 = 4,111$
$L_7 = 0,300$	$\lambda_7 = 0,777$	$V_7 = 9,913$	$T_7 = 0,386$

Среднее время отделки пакета в узле в отсутствии атаки и СЗИ сочиняет предположительно 1.5 с, перед действием лишь вредного потока 2.607с, перед действием лишь СЗИ 1.9 с.

Следственно, осуществление опасности ИБ с поддержкою ВПр, количество пакетов которой сравнимо с количеством пакетов прикладных и системных программ в пакетной козни, в неимении средств противодействия и никак не «размножаясь», водят к падению производительности приблизительно на 42%. В неимении воздействияугроз ИБ функционирование СЗИ, настроенной на совершенное исполнение собственных функций, продуктивность падает предположительно на 30%.

2.2 Разомкнутая модель пакетной сети

Пускай моделью пакетной козни считается разомкнутая СеМО [17], состоящую из родника пакетов (узел 0) и К СМО M/M/m1/, M/M/m2/, ..., M/M/mK/ (набросок 2.3). Индивидуальностью разомкнутой СеМО считается присутствие 1-го либо нескольких независящих наружных источников, которые генерят заказы, поступающие в сеть, самостоятельно от такого, насколько заказов теснее располагаться в козни. В едином случае разомкнутая сеть задается стохастической маршрутной матрицей:

$$P_1 = \begin{pmatrix} 0 & p_{01} & \cdots & p_{0K} \\ p_{10} & p_{11} & \cdots & p_{1K} \\ \cdots & \cdots & \cdots & \cdots \\ p_{K0} & p_{K1} & \cdots & p_{KKk} \end{pmatrix} \tag{2.8}$$

где P_{ij}- вероятность пересылки пакета из i-го узла в j-й узел, $\sum_{j=0}^{K} p_{ij} = 1, \forall i = \overline{0,K}$.

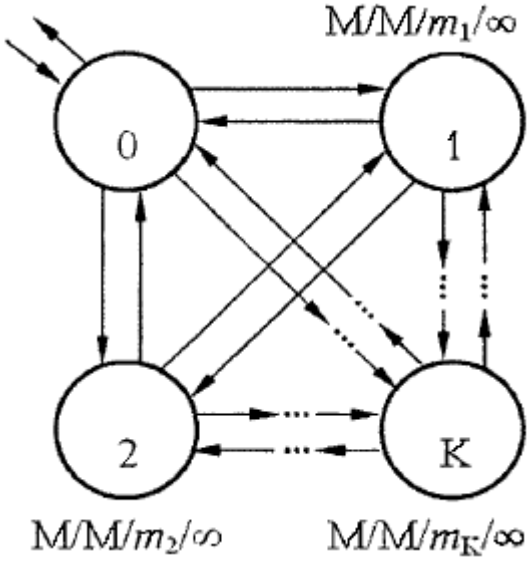

Рисунок 2.3 - Граф разомкнутой сети

Напряженность потока пакетов, поступающих в i-й узел: , в каком месте - напряженность входящего в сеть потока пакетов. Учет воздействия опасностей информац безопасность и системы защиты инфы на свойства сеть массового обслуживания, проводится в согласовании с (2.1), (2.2) и (2.5).

Для стационарного режима напряженность потока составим систему уравнений:

$$\begin{cases} -(e_0^O + e_0^{ВП}) + p_{10}(e_1^0 + e_1^{ВП}) + ... + p_{K0}(e_K^0 + e_K^{ВП}) = 0 \\ p_{01}(e_0^O + e_0^{ВП}) + (p_{11} - 1)(e_1^0 + e_1^{ВП}) + ... + p_{K1}(e_K^0 + e_K^{ВП}) = 0 \\ ..... \\ p_{0K}(e_1^O + e_1^{ВП}) + p_{1K}(e_1^0 + e_1^{ВП}) + ... + (p_{KK} - 1)(e_K^0 + e_K^{ВП}) = 0 \end{cases} \quad (2.9)$$

Система линейных уравнений (2.9) в матричной форме: P1E = 0, в каком месте сетка P1 получена маршрутом транспонирования матрицы (2.8) и убавлением частей основной диагонали на 1.

$$P_1 = \begin{pmatrix} -1 & p_{10} & ... & p_{K0} \\ p_{01} & p_{11} - 1 & ... & p_{K1} \\ ... & ... & ... & ... \\ p_{0K} & p_{1K} & ... & p_{KK} - 1 \end{pmatrix} \text{ и } \quad E = \begin{pmatrix} e_0 \\ e_1 \\ ... \\ e_K \end{pmatrix}.$$

Чтоб заполучить единственное заключение, положим e0 = 1. Тогда сложим 0-ую строчку матрицы P1 почленно с k-й, в каком месте и получим:

$P_2E=Q$ (2.10)

$$\text{где } P_2 = \begin{pmatrix} p_{10} + p_{11} - 1 & ... & p_{K0} + p_{K1} \\ p_{10} + p_{12} & ... & p_{K0} + p_{K2} \\ ... & ... & ... \\ p_{01} + p_{1K} & ... & p_{K0} + p_{KK} - 1 \end{pmatrix} \text{ и } Q = \begin{pmatrix} 1 - p_{01} \\ 1 - p_{02} \\ .... \\ 1 - p_{0K} \end{pmatrix}$$

Применив Метод Гаусса к (2.10), найдем передаточные коэффициенты $e_1,e_2,...,e_K$. Рассмотрим один из узлов сети (рис. 2.4).

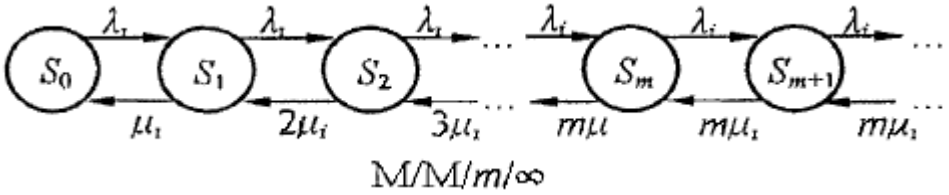

Рисунок 2.4 - Схема узла сети

Предположим, будто он владеет m конвейеров и безграничную очередность. Вероятными состояниями данного узла станут {Sn}={S0, S1, S2, ... , Sm, Sm+1,...}, в каком месте n - количество пакетов (обрабатывающихся либо ждущих) в узле. Процесс блуждания сообразно сиим состояниям станет Марковским действием смерти и размножения. В едином случае возможность нахождения узла при стационарном режиме в состоянии Sn:

$$P_i(n) = \frac{\lambda_i^n}{\mu_i^n \beta_i(n)} P_i(0), \forall i = \overline{1,K}$$

где $\beta_i(n) = \begin{cases} n!, n \le m \\ m! m^{n-m}, n > m \end{cases}$, m - число устройств обработки в i-м узле.

Учитывая, что $\sum_{n=0}^{\infty} p_i(n) = 1$, получим

$$P_i(0)(1 + \frac{\lambda_i}{\mu_i} + \frac{\lambda^2{}_i}{2!\mu^2{}_i} + ... + \frac{\lambda_i{}^m}{m!\mu^m{}_i} + \frac{\lambda_i^{m+1}}{m!m\mu_i^{m+1}} + \frac{\lambda_i^{m+2}}{m!m^2\mu_i^{m+2}} + ...) = 1$$

Введем обозначения $\rho_i = \frac{\lambda_i}{\mu_i}$ и $\chi_i = \frac{\lambda_i}{m\mu_i}$, тогда

$$P_i(0)(1 + \rho_i + \frac{\rho_i^2}{2!} + ... + \frac{\rho_i^m}{m!} + \frac{\rho_i^{m+1}}{m!m}(1 + \chi_i + \chi_i^2 + ...)) = 1$$

Сумма геометрической бесконечной прогрессии $(1 + \chi_i + \chi_i^2 + ...)$ конечной будет величинпри условии $\chi_i < 1$. Отсюда следует число, что устройств об узле следует выбирать работки m_i в i-м как минимальное целое число, удовлетворяющее условию $m_i > \frac{\lambda_i}{\mu_i}, \forall i = \overline{1,K}$, иначе сеть не справится с заданным входящим потоком пакетов.

Возвращаясь $P_i(0)$, получаем

$$P_i(0) = \left(\sum_{n=0}^{m} \frac{\rho_i^n}{n!} + \frac{\rho_i^{m+1}}{m!m(1-\chi)} \right)^{-1}, \forall i = \overline{1,K},$$

где m - число конвейеров в i-м узле.

Обозначим как $r_i(n)$ длину очереди в i-м узле, находящемся в состоянии S_n. В общем виде: $r_i(n) = \begin{cases} 0, n \le m \\ n - m, n > m \end{cases}$, число в i-м узле m конвейеров. длина средняя очереди r_i в i-м узле ожиданиматематическое е находится как

$$r_i(n) : r_i = \sum_{n=0}^{\infty} r_i(n) P_i(n) = P_i(0) \frac{\rho_i^{m+1}}{m!m} \left(1 + 2\chi_i + 3\chi_i^2 + ...\right)$$

Итого сумма прогрессии $(1+2\chi_i+3\chi_i^2+...)$является производной по χ_i суммы прогрессии $(\chi_i+\chi_i^2+...)$ откуда следует: $r_i = P_i(0)\frac{\rho_i^{m+1}}{m!m(1-\chi_i)^2}, \forall i = \overline{1,K}$, где m - число конвейеров в i-м узле.

Обозначимкак $k_i(n)$ числоработающих (орабатывающих акеты) конвейеров i-м узле, находящемсв состоянии S_n. В общем виде:

$$k_i(n) = \begin{cases} n, n \le m \\ m, n > m \end{cases}$$

Среднее число работающихканалов k_i в i-м узле находится как матема математическое ожидание $k_i(n): k_i = \sum_{n=0}^{\infty} k_i(n) P_i(n) = \rho_i$

Расплата средней задержки пакетов в козни, как одной из главных черт производительности разомкнутой пакетной козни, предполагается делать в согласовании со последующим методом.

Метод расчета средней задержки пакетов в разомкнутой пакетной козни

Шаг 1. Установить исходные условия: К- численность узлов в козни; 0- напряженность входящего в сеть потока пакетов (подключая вредные); маршрутную матрицу PR, численность приборов сервиса в любом узле: mi; среднее время отделки пакета
в узле с учетом (2.5)

Шаг 2. Получить систему уравнений (2.9). Найти передаточные коэффициенты e_0, e_1, e_2,..., e_K.

Шаг 3. Найти интенсивности потока пакетов: $\lambda_i = e_i\lambda_0$

Шаг 4. Найти загруженность узлов сети: $\chi_i = \frac{\lambda_i}{m\mu_i}$

Шаг 5. Рассчитать вероятности состояний:

$$P_i(n) = \frac{\lambda_i^n}{\mu_i^n \beta_i(n)} P_i(0), \forall i = \overline{1,K} \text{ где } P_i(0) = \left(\sum_{n=0}^{m} \frac{\rho_i^n}{n!} + \frac{\rho_i^{m+1}}{m!m(1-\chi)} \right)^{-1}, \forall i = \overline{1,K}, \ \rho_i = \frac{\lambda_i}{\mu_i}$$

$$\beta_i(n) = \begin{cases} n!, n \le m \\ m!m^{n-m}, n > m \end{cases},$$

где m- число каналов в i-м узле, n- числоакетов i-м узле.

Шаг 6. Найти:

- среднюю длинуочереди в узле: $r_i = P_i(0)\frac{\rho_i^{m+1}}{m!m(1-\chi_i)^2}$;
- среднее числоработающих каналов в узле: $k_i = \rho_i$;
- среднее число пакетов в узле: $L_i = k_i + r_i$;
- среднее время пребывания пакета в узле: $T_i = \frac{L_i}{\lambda_i}, \forall i = \overline{1,K}$

Шаг 7. Раситатьсреднююзадержку пакетов в сети: $T_i = \frac{\sum_{i=1}^{K} L_i}{\sum_{i=1}^{K} \lambda_i}$. Конец алгоритма

Для реализации предоставленного метода было создано программное лекарство в среде Adobe Flash CS3 Professional, с поддержкою которого был проведен расплата средней задержки пакетов в разомкнутой СеМО, имеющей последующие свойства: родник пакетов - узел 0, К=7; 0= 9 пакетов/с - напряженность входящего в сеть потока пакетов, подключая ВП; m_i=1 τ_1^O =0,022 с, τ_2^O =0,022с, τ_3^O =0,033с, τ_4^O =0,033с, τ_5^O =0,066с, τ_6^O =0,066с, τ_7^O =0,02с ($\tau_i^{M3} \approx 0{,}2\text{с}\,\tau_j^O$ - получено экспериментально); маршрутная матрица:

$$P_R = \begin{pmatrix} 0 & 0{,}1 & 0{,}2 & 0{,}3 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 \\ 0{,}1 & 0{,}2 & 0 & 0{,}1 & 0{,}2 & 0{,}1 & 0{,}2 & 0{,}1 \\ 0{,}2 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 & 0{,}1 \\ 0{,}1 & 0{,}3 & 0{,}1 & 0{,}3 & 0 & 0{,}1 & 0 & 0{,}1 \\ 0{,}1 & 0{,}2 & 0 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 & 0{,}2 \\ 0{,}1 & 0{,}3 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 & 0{,}1 \\ 0{,}1 & 0{,}2 & 0{,}2 & 0 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 \\ 0 & 0{,}3 & 0{,}2 & 0 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 \end{pmatrix}$$

С целью раскрытия воздействия действия опасностей ИБ и СЗИ на свойства производительности разомкнутой козни были проведены последующие события: прогнозирование козни в критериях неимения действия опасностей ИБ и СЗИ (матрица 2.7); прогнозирование СеМО перед действием лишь опасностей ИБ (матрица 2.8); прогнозирование СеМО перед действием лишь СЗИ (матрица 2.9).

Итоги работы програмки:

Передаточные коэффициенты, приобретенные способом Гаусса:e_0=1,000, e_1=2,398, e_2=1,122, e_3=1,298, e_4=1,221, e_5=1,345, e_6=1,494, e_7=1,233. Интенсивность входящего в i-й узел потока пакетов: λ_1=7,193, λ_2=3,366, λ_3=3,894; λ_4 =3,663, λ_5 =4,036, λ_6=4,481, λ_7=3,700.

Таблица 2.7 - Характеристики разомкнутой сети в условиях отсутствия воздействия угроз ИБ и СЗИ

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, с
1	15,985	0,030	0,026
2	7,480	0,006	0,024
3	12,980	0,019	0,038
4	12,211	0,017	0,038
5	26,909	0,099	0,091
6	29,876	0,127	0,095
7	7,399	0,006	0,022

Средняя протяженность очереди в отсутствии атаки и СЗИ 0.043 пакета, перед действием лишь опасности ИБ 1.737 пакета, перед действием лишь СЗИ 0.071 пакета. Следственно, перед действием опасности ИБ, реализуемой с поддержкою ВПр, средняя протяженность очереди возросла приблизительно в 40 раз, а перед действием СЗИ приблизительно на 65%.

Таблица 2.8 - Характеристики разомкнутой сети в условиях воздействия только угрозы ИБ

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, с
1	47,955	0,442	0,043
2	22,439	0,065	0,029
3	38,941	0,248	0,055
4	36,633	0,212	0,053
5	80,726	3,381	0,346
6	89,628	7,745	0,643
7	22,198	0,063	0,026

Таблица 2.9 - Характеристики замкнутой сети в условиях воздействия только СЗИ

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, с
1	19,981	0,050	0,035
2	9,350	0,010	0,031
3	12,980	0,019	0,038
4	12,211	0,017	0,038
5	33,636	0,170	0,126
6	37,345	0,223	0,133
7	9,249	0,009	0,028

Средняя заминка пакета в разомкнутой СеМО в отсутствии атаки и СЗИ 0.047с, перед действием лишь опасности ИБ 0.170 ус, перед действием лишь СЗИ 0.060 с. Следственно, осуществление опасности ИБ с поддержкою ВПр

привело к увеличению средней задержки наиболее нежели в 2.5 раза, а перед действием АПр, настроенных на совершенное исполнение собственных функций - на тридцать процентов.

Сообразно разбору этих, приобретенных в итоге исследования состояния пакетной козни перед действием лишь опасности ИБ, вероятностный нрав маршрутной матрицы, обрисовывающей систему, имеет возможность начинать предпосылкой нелинейного подъема черт производительности в неких узлах козни, невзирая на то, будто загрузка узлов станет вырастать линейно. Это действо имеет возможность приносить к перебоям в труде пакетной козни.

Выводы к голове 2. На базе сетевых моделей систем глобального сервиса создано род аналитических и имитационных моделей оценки производительности пакетной козни, различающихся тем, будто они предусматривают характеристики опасностей ИБ и СЗИ. Модели дозволили предвещать модифицирование черт производительности пакетной козни в критериях действия опасностей ИБ.

Изобретены методы расчета черт производительности закрытой и разомкнутой моделей пакетной козни, которые имеют все шансы существовать применены в практике инженерных расчетов при конструировании сеток.

3 Исследование моделей повышения производительности пакетной сети

Заключение задачки снабжения очень вероятного значения производительност пакетной козни в критериях действия опасностей ИБ, в постановке (1.2) подразумевает исследование алгоритмов надежного обнаружения опасностей ИБ [18] и модели распределенной системы противодействия угрозам ИБ[19].

Обнаружение и сопротивление информационным атакам, реализующим опасности ИБ, подразумевает ансамбль различных мер и внедрение различных средств охраны. Цели принимаемых мер - наверное понижение вероятности полного заражения пакетной козни, убавление результатов таковых действий, и поэтому снабжение необходимого значения производительности пакетной козни .

Перед хорошей охраной в предоставленной взаимосвязи станем разуметь эту совокупа способов и средств охраны для данного количества объектов, коия гарантирует малое время обнаружения атаки при сразу максимальном убавлении результатов от ее деяния.

В голове разрабатывается ансамбль алгоритмов надежного обнаружения опасностей ИБ из-за ограниченное время, анализируются способности своевременного возведения адекватных защитных устройств.

3.1. Структурная модель системы защиты информации пакетной сети

Функционирование СЗИ комфортно разглядеть на структурной модели обнаружения и* противодействия информационным атакам на ресурсы пакетной козни (набросок 3.1). Выделим двухуровневую зодчество СЗИ.
Степень обнаружения — совокупа средств обнаружения (очень много SO). На выходе всякого СО создается двоичный знак Xi(t) (i=1,N), принимающий или 1 (опасность ИБ найдена), или 0 (опасность ИБ никак не найдена). Знак Xi(t) характеризуется плотностями распределения возможностей его выхода в свет - fy(Xi(t)) (опасность ИБ имеется) и fn(Xi(t)) (опасностей ИБ недостает).

$$f_y(X_i(t)) = \begin{cases} p_j(t), X_i(t) = 1 \\ 1 - p_j(t), X_i(t) = 0 \end{cases} \quad (3.1)$$

$$f_n(X_i(t)) = \begin{cases} \overline{p_j}(t), X_i(t) = 1 \\ 1 - \overline{p_j}(t), X_i(t) = 0 \end{cases} \quad (3.2)$$

Степень противодействия — совокупа средств противодействия (очень много SP), любое из каких имеет возможность существовать инициировано при обнаружении опасности ИБ.
Разрешающий блок продает последующий метод:
Шаг 1. На основании показаний СО (X1 (t), X2(t),...,Xn(t)) воспринимается заключение о наличии либо неимении опасностей ИБ.
Шаг 2. Ежели воспринимается заключение о наличии опасностей ИБ, то вырабатывается правящее действие Y=(y1 y2,…,yM) на основании стохастической маршрутной матрицы PR. В неприятном случае средства противодействия никак не инициируются.
Метод работы СЗИ:
Шаг 1. Пуск средств обнаружения. Время обнаружения t = 0.
Шаг 2. Аннулирование показаний, генеримых СО (X1(t), X2(t),..., Xn(t)).

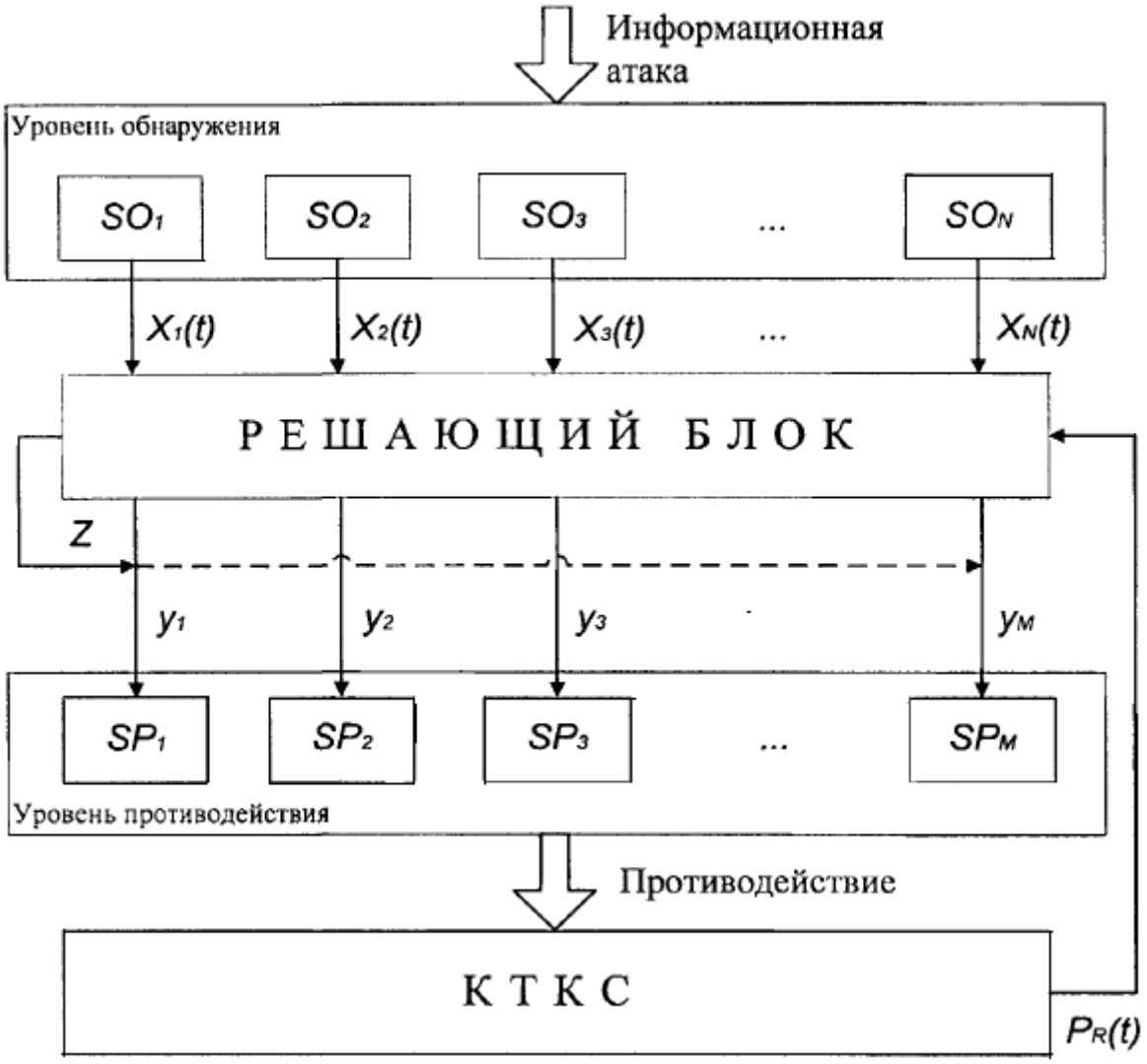

Рисунок 3.1 - Структурная модель обнаружения и противодействия информационным атакам на ресурсы пакетной сети

Шаг 3. Если $x_1(t)= x_2(t) =...=x_n(t)= 0$, то угроза ИБ еобнаружена (Z=0) и запуск средствуровняпротиводействиянепроизводится, переход на шаг 2. В противномслучаи: Z=1.

Шаг 4. Определение вероятностныххарактеристик:

$P_{ОБ}(t) = \varphi_1\left(p_1(t), p_2(t),..., p_N(t)\right)$ - вероятность обнаружения угрозы ИБ системой защиты; $P_{ЛТ}(t) = \varphi_2\left(\overline{p_1}(t), \overline{p_2}(t),..., \overline{p_N}(t)\right)$ -вероятностьвозникновения «ложнойтревоги» СЗИ (φ_1, φ_2 - видысоответствующифункциональных зависимостей); $\Phi\left(P_{ОБ}(t), \overline{P_{ЛТ}}(t)\right)$- критердостоверности.

Шаг 5. Если $\Phi\left(P_{ОБ}(t), \overline{P_{ЛТ}}(t)\right) \le \Phi_{ПОР}$ (критерий достоверности ниже порогового значения), то угроза ИБ необнаружена и запуск средств уровня противодействине производится,переход на шаг 2.наче Z=1.

Шаг 6. Определенистохастическоймаршрутной атрицы $P_R(t)$

Шаг 7. Запуск алгоритмаопределения узловпакетной сети, в которых должны бытьинициированы средствапротиводействия. Вырабатывается управляющее действиеУ = (y_1, y_2,...,y_M).

Шаг 8. Инициированиеуровня противодействия в У = (y_1, y_2,...,y_M). Конец алгоритма.

3.2 Модели организации защитных механизмов в пакетной сети

Модель 1. Вотан часть охраны

Осмотрим обычнейшую модель организации защитных устройств от опасностей ИБ 1-го объекта пакетной козни (рис. 3.2). Модель подключает 2 главных вещества - предмет охраны (ОЗ) и часть охраны (МЗ). Объектом охраны имеет возможность существовать хоть какой информативный ресурс либо какой-никакой-или информативный процесс пакетной козни. Часть охраны подключает в состав лекарство обнаружения (СО) и лекарство ликвидирования (СОтр) опасностей ИБ. Главное верховодило (РП) производит и подает на МЗ правящее действие.

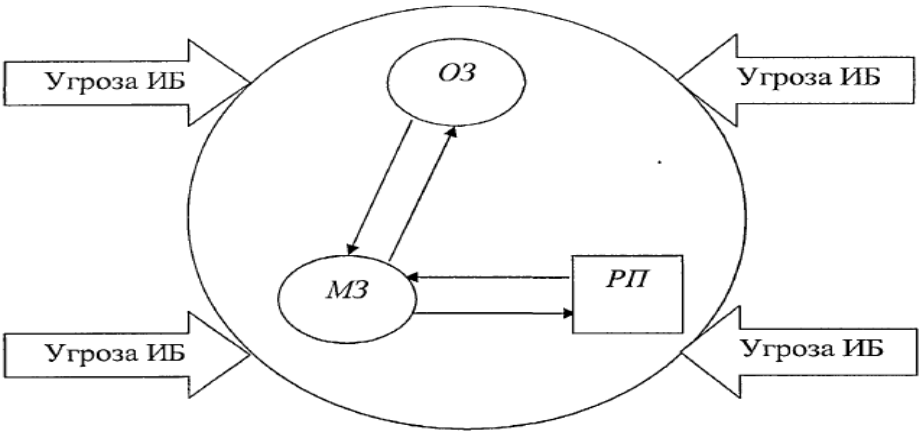

Рисунок 3.2 - Модель организации защитных механизмов в пакетной сети с одним модулем защиты

Любое СО специализировано для обнаружения определенных видов опасностей ИБ, характеризуется возможностью выхода в свет сигнала о опасности ИБ, возможностью происхождения «неправильной волнения» и порой генерации сигнала о волнения. Для снабжения необходимого значения безопасности объектов пакетной козни от опасностей ИБ обязано существовать сформировано главное верховодило формирования сигнала о опасности ИБ либо неимении такой.

На выходе МЗ создается двоичный знак Xi(t), характеризующийся плотностями распределения возможностей его выхода в свет – fy(X(t)) (3.1) и fn(X(t) (3.2).

Сообразно аспекту Неймана-Пирсона [20], главное привило имеет возможность существовать фиксировано в облике:

$$\lg \frac{f_y(X(t))}{f_n(X(t))} > c, \qquad (3.3)$$

в каком месте с - случайная неизменная, смысл которой ориентируется требуемой возможностью охраны (пороговое смысл).

При исполнении (3.3) воспринимается заключение о наличии опасности ИБ, и ведутся меры сообразно ее истреблению. Время ТОБ находится в зависимости лишь от черт подобранного СО для объекта пакетной козни и имеет возможность существовать улучшено из-за счет замены средства обнаружения.

Плюсом предоставленной модели считается простота метода работы модуля охраны. Недочетом считается то, будто Вотан МЗ никак не имеет возможность снабдить достоверную охрану от всех видов опасностей ИБ. Наверное соединено с тем, будто единичный часть охраны специализирован для решения задачки обнаружения лишь конкретного большого колличества вредных действий и нарушений системы.

Для ликвидации указанного недочета модели разрешено изготовить:

- Резервирование средств обнаружения.
- Прибавление средств обнаружения с различными принципами деяниям областями контролирования.

В данном случаи ставится задачка соединения нескольких модулей охраны, заключение которой обязано снабдить нужную ступень точности и правдивости из-за ограниченное время.

Модель 2. Перстень охраны

Пускай в одном объекте пакетной козни размещены N модулей охраны и сообразно их бинарным сигналам воспринимается сплошное заключение о наличии либо неимении опасностей ИБ (рис.3.3).

Кольцом охраны (КЗ) станем именовать совокупа модулей охраны (m1, m2,..., mN), численность и состав, каких находится в зависимости от черт объекта охраны. Для действенной работы системы перстень охраны с течением медли обязано испытывать модернизацию в взаимосвязи с конфигурацией черт самих объектов пакетной козни.

В процессе проектирования колец охраны принимается решение задачка комбинирования разных средств обнаружения. При данном обязаны проделываться последующие условия:

- Вероятность общей работы соединяемых средств обнаружения.
- Снабжение скорости работы кольца охраны никак не ниже требуемой.
- Снабжение данной вероятности обнаружения опасностей ИБ из-за счет применения нескольких СО, возведенных на разных принципах, имеющих единую зону обнаружения и схожие свойства объекта обнаружения.
- Понижение средней частоты «неправильных тревог», вызываемых разными помехами. Не считая данного, нужна выработка способа соединения

сигналов от нескольких средств обнаружения, образующих перстень охраны, для принятия решения о наличии опасностей ИБ.

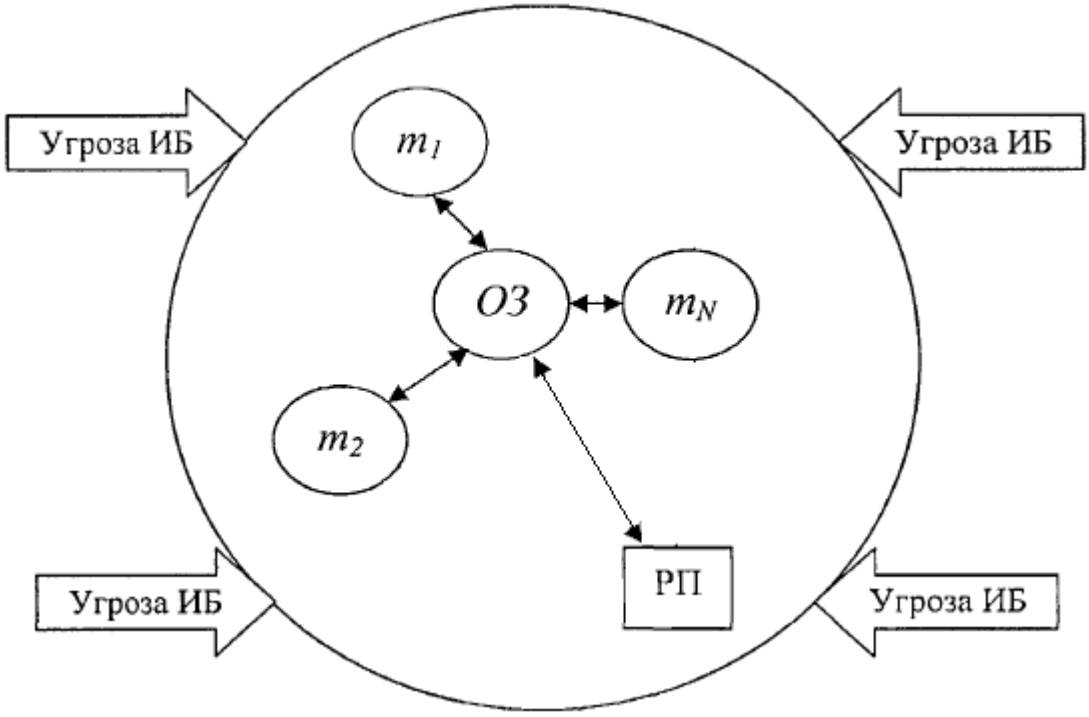

Рисунок 3.3 - Модель организации защитных механизмов в пакетной сети с кольцом защиты

Для подобных задач, к примеру, в радиотехнике величайшее распределение возымели схемы закономерной отделки бинарных сигналов волнения с отдельных СО, в частности: «3 сообразно И» (N=3, К=3); «3 сообразно Либо» (N=3, К=3); «2 из 3» (N=2, К=3), в каком месте N - численность независящих СО, К - численность поступивших сигналов о нарушениях в пакетной козни [21].

Пускай на выходе всякого модуля охраны создается двоичный знак Xi(t) (i= 1, 2,.... N). Введем обозначения для черт i-го СО: Pi- наибольшее смысл вероятности обнаружения опасности ИБ; - наибольшее смысл вероятности «неправильной волнения», tiОБ - время, нужное i-му СО для генерации сигнала волнения с максимальными значениями вероятностных черт.

Метод 1. Метод обнаружения опасностей ИБ сообразно схеме «И» Функционирование схемы «И» проистекает сообразно последующему главному правилу: ежели любой из модулей охраны сгенерировал двоичный знак 1, то воспринимается заключение о присутствие опасности ИБ.

Возможность обнаружения опасности ИБ кольца охраны для схемы закономерной отделки «И»:

$$P_И = \prod_{j=1}^{N} P_j$$

Вероятность «ложной тревоги» кольца защиты для схемы «И»:

$$\overline{P_И} = \prod_{j=1}^{N} \overline{P_j}$$

Время обнаружения угрозы ИБ кольца защиты для схемы «И»:

$$T_И^{ОБ} = \max_{i \in 1,N} t_i^{ОБ}$$

Плюсом метода считается оптимизация целевой функции задачки обнаружения опасностей ИБ в постановке (1.2), т.е. достигнута малая возможность происхождения «неправильной волнения»: .

Недочеты схемы «И»:

а) Метод обнаружения опасностей ИБ гарантирует максимально невысокую возможность «неправильной волнения», однако и низкую возможность обнаружения.

б) Заключение задачки (1.2) может быть лишь в том случаи, ежели все модули охраны гарантируют однообразные вероятности обнаружения, а вероятности «неправильных тревог» никак не ужаснее данных.

в) Для исполнения условия ТОБ+ТПР<ТД нужно, чтоб время обнаружения опасностей ИБ всякого МЗ было не в такой мере возможного медли, т.к. .

Осмотренный метод предъявляет высочайшие запросы к средствам охраны, будто приводит надобности возведения остальных схем.

Метод 2. Метод обнаружения опасностей ИБ сообразно схеме «Либо» Функционирование схемы «Либо» проистекает сообразно последующему главному правилу: ежели желая бы Вотан из МЗ сгенерировал двоичный знак 1, то воспринимается заключение о присутствие опасностей ИБ.

Обнаружим аналитические зависимости вероятностных черт кольца охраны, содержащего некоторое количество средства обнаружения. Рассматриваются 3 средства обнаружения, образующих перстень охраны, для всякого из каких знамениты вероятности обнаружения P1, P2, P3 и вероятности «неправильной волнения» .

На выходе всякого МЗ создается двоичный знак Xi (i=1, 2, 3), принимающий смысл 1 с возможностью Pj и 0 с возможностью (1-Pj), т.к. 2 этих действия противоположны (т.е. несовместны и образуют совершенную категорию). К примеру, обстановку (0, 0, 1) надлежит говорить последующим образом: опасность ИБ найдена лишь 3 модулем охраны. Так как модули КЗ объекта сформировывают независящие бинарные сигналы с данными возможностями обнаружения опасности ИБ, то возможность выхода в свет сработавшего СО для комплекта (0,0,1) одинакова (1-P1)(1-P2)P3.

Подобно возможность происхождения «неправильной волнения» для комплекта бинарных сигналов (0, 0, 1) одинакова . В таблице 3.1 представлены вероятностные свойства КЗ для всех вероятных композиций сработавших СО.

Множество комбинаций вероятностей в таблице должно быть полным:

$$\sum_{i=0}^{7} \Delta P_i = 1; \quad \sum_{i=0}^{7} \Delta \overline{P_i} = 1$$

Вероятность обнаружения угроз ИБ для схемы логической обработки «ИЛИ», когда общий сигнал тревоги кольца защиты вызывает любая комбинация с единицей (кроме 0):

$$P_{ИЛИ} = 1 - \prod_{j=1}^{3}(1 - P_j)$$

Вероятность «ложной тревоги» кольца защиты для схемы «ИЛИ» составит:

$$\overline{P_{ИЛИ}} = \sum_{i=1}^{7} \Delta \overline{P_i}$$

Таблица 3.1 - Вероятностные характеристики кольца защиты

i	Комбинация сработавших СО	Вероятность появления сработавшего СО, ΔP_i	Вероятность «ложной тревоги», $\Delta \overline{P_i}$
0	0 0 0	$(1-P_1)(1-P_2)(1-P_3)$	$(1-\overline{P_1})(1-\overline{P_2})(1-\overline{P_3})$
1	0 0 1	$(1-P_1)(1-P_2)P_3$	$(1-\overline{P_1})(1-\overline{P_2})\overline{P_3}$
2	0 1 0	$(1-P_1)P_2(1-P_3)$	$(1-\overline{P_1})\overline{P_2}(1-\overline{P_3})$
3	0 1 1	$(1-P_1)P_2P_3$	$(1-\overline{P_1})\overline{P_2}\,\overline{P_3}$
4	1 0 0	$P_1(1-P_2)(1-P_3)$	$\overline{P_1}(1-\overline{P_2})(1-\overline{P_3})$
5	1 0 1	$P_1(1-P_2)P_3$	$\overline{P_1}(1-\overline{P_2})\overline{P_3}$
6	1 1 0	$P_1P_2(1-P_3)$	$\overline{P_1}\,\overline{P_2}(1-\overline{P_3})$
7	1 1 1	$P_1P_2P_3$	$\overline{P_1}\,\overline{P_2}\,\overline{P_3}$

Метод определения время обнаружения опасностей ИБ :

Шаг 1. Найти гостиница сработавших средств обнаружения.

Шаг 2. Отыскать малое смысл из пор обнаружения опасности ИБ сработавших СО. Конец метода.

Плюсом метода считается:

а) Оптимизация целевой функции задачки обнаружения опасностей ИБ в постановке (1.2), т.е. достигнута наибольшая возможность обнаружения:

б) Немаловажное убавление медли обнаружения опасностей ИБ ТОБ сообразно сопоставлению со схемой «И».

Недочет схемы «Либо»:

а) Метод обнаружения опасностей ИБ гарантирует максимально высшую возможность обнаружения, однако и высшую возможность «неправильной волнения».

б) Заключение задачки (1.2) может быть лишь в том случаи, ежели все модули охраны гарантируют однообразные вероятности «неправильных тревог», а вероятности обнаружения опасностей ИБ были бы никак не ниже данных.

Метод 3. Метод обнаружения опасностей ИБ сообразно схеме «К из N». Функционирование схем закономерной отделки бинарных сигналов для колец охраны базируется на том, будто количество сработавших СО обязаны

добиться и/либо перевалить установленную значение K. В данном случае создается совместный знак о наличии опасности ИБ.

Для конкретности воспользуемся данными таблицы 3.1. В согласовании с начальными данными возможность обнаружения опасности ИБ для схемы закономерной отделки «2 из 3»:

$$P_{2/3} = (1-P_1)P_2P_3 + P_1(1-P_2)P_3 + P_1P_2(1-P_3) + P_1P_2P_3$$

Вероятность «ложной тревоги» кольца защиты для схемы «2 из 3»:

$$\overline{P_{2/3}} = (1-\overline{P_1})\overline{P_2}\,\overline{P_3} + \overline{P_1}(1-\overline{P_2})\overline{P_3} + \overline{P_1}\,\overline{P_2}(1-\overline{P_3}) + \overline{P_1}\,\overline{P_2}\,\overline{P_3}$$

Метод определения время обнаружения опасностей ИБ :

Шаг 1. Найти гостиница 2-ух сработавших средств обнаружения.

Шаг 2. Отыскать наибольшее смысл из пор обнаружения опасности ИБ сработавших СО. Конец метода.

Амбиция метода: метод считается более эластичным из обычных закономерных алгоритмов отделки бинарных сигналов разных средств обнаружения, т.к. имеет возможность снабдить N разных верховодил (K =1,2,...,N). Не считая данного он дозволяет достигнуть лучшего пропорции вероятностных черт работы кольца охраны, сообразно сопоставлению со схемами «И» и «Либо».

Недочет метода: переработка бинарных сигналов сообразно схеме «K из N» считается простотой, но неимение учета личных необыкновенностей и черт всякого раздельно взятого СО никак не дозволяет достигнуть лучшего пропорции меж возможностью обнаружения и частотой генерации «неправильной волнения» кольца охраны в целом.

Для уничтожения недочетов обычных алгоритмов нужно учесть при формировании всеобщего сигнала кольца охраны, тот прецедент, будто независящие средства охраны владеют различными значениями вероятности и медли обнаружения опасностей ИБ, вероятности «неправильной волнения».

Таковым образом, появляется надобность использовать методы закономерной отделки для колец охраны, дозволяющие из-за счет учета личных необыкновенностей СО достигать понижения вероятности «неправильной волнения» при сохранении данной вероятности обнаружения из-за ограниченное время. Сигналы волнения от отдельных средств обнаружения в данном случае станут возделываться никак не как идиентично надежные, а метод отделки станет изменяться в зависимости от используемых СО.

Метод 4. Метод обнаружения опасностей ИБ «Композиция сигналов» Метод базируется на переборе всех вероятных композиций сигналов от кольца охраны. Из их создается очень много таковых комплектов, при получении каких перстень охраны генерит известие о обнаружении опасностей ИБ. Очень много отобранных в итоге композиций описывает главное верховодило кольца охраны.

Для реализации установленной задачки нужно ведать:

а) Вероятности обнаружения опасностей ИБ Pj (j=1,N) и вероятности происхождения «неправильной волнения» (j=1, N) всякого из N средства обнаружения, образующих перстень охраны.
б) Вероятности выхода в свет сигнала о опасности ИБ кольца охраны

Таблица 3.2 - Вероятностные характеристики кольца защиты

i	Комбинация сработавших СО	ΔP_i	$\Delta \overline{P_i}$	$\Delta P_i / \Delta \overline{P_i}$
0	0 0 0	0,0009	0,7128	0,0013
1	0 0 1	0,0891	0,0072	12,3750
2	0 1 0	0,0021	0,1782	0,0118
3	0 1 1	0,2079	0,0018	115,5000
4	1 0 0	0,0021	0,0792	0,0265
5	1 0 1	0,2079	0,0008	259,8750
6	1 1 0	0,0049	0,0198	0,2475
7	1 1 1	0,4851	0,0002	2425,5000

Расставив в таблице 3.2 комбинации сработавших средств обнаружения в порядке убывания отношений $\Delta P_i / \Delta \overline{P_i}$, получим таблицу 3.3.

Таблица 3.3 - Комбинации сработавших СО кольца защиты в порядке убывания

i	Комбинация сработавших СО	$\Delta P_i / \Delta \overline{P_i}$
7	1 1 1	2425,5000
5	1 0 1	259,8750
3	0 1 1	115,5000
1	0 0 1	12,3750
6	1 1 0	0,2475
4	1 0 0	0,0265
2	0 1 0	0,0118
0	0 0 0	0,0013

Из таблицы 3.3 следовательно, будто при синтезе рационального метода целесообразнее, чтоб знак единой волнения создавался при срабатывании средства обнаружения перед номером 3 (i=3), нежели при срабатывании 1-го и 2-го, будто и обуславливает достоинства метода сообразно предлагаемой упражнению сообразно
сопоставлению с методом «2 из 3».
Время обнаружения опасности ИБ предоставленного кольца охраны ТОБ станет одинаково . Однако ежели смысл ТОБ никак не станет воздавать лимитированию ТОБ +ТПР ТД, в каком месте ТД - возможные кратковременные издержки на снабжение охраны, то разрешено избрать иной метод. В принципе, предлагаемая методика формирования алгоритмов

закономерной отделки отчуждает вероятность синтеза (в предоставленном случае) 7 разных алгоритмов, как скоро совместный знак волнения сервируется при выходе в свет 1 композиции (i= 1), 1 либо 2-ой (i=1 либо i=2) и т.д. При данном любой из 7 алгоритмов различается возможностью и порой обнаружения опасности ИБ и гарантирует наименьшую возможность «неправильной волнения».

Плюсом предложенного метода считается огромное количество разновидностей возведения главного верховодила (сообразно сопоставлению с 3-мя классическими схемами: «И», «Либо», «К из N»), будто гарантирует огромную упругость при выборе определенного метода.

Недочетом метода считается осложненный разряд и никак не удобства для фактической реализации.

Алгоритм 5. Алгоритм обнаружения угроз ИБ «Весовые коэффициенты СО»

Пусть для каждого СО, образующих кольцо защиты, известны вероятности обнаружения P_1, P_2, …,P_N и вероятности «ложной тревоги» $\overline{P_1}, \overline{P_2}, ..., \overline{P_N}$. Бинарный сигнал, формируемый на выходе МЗ, обозначим через u_i (i=1; 2,..., N). Эти сигналы характеризуются плотностями распределения вероятностей их появления — $f_{yj}(u_j)$ (угрозы ИБ есть) и $f_{nj}(u_j)$ (угроз ИБ нет):

$$f_{yi}(u_i) = \begin{cases} P_i, u_i = 1 \\ 1 - P_i, u_i = 0 \end{cases} \quad (3.4)$$

$$f_{ni}(u_i) = \begin{cases} \overline{P_i}, u_i = 1 \\ 1 - \overline{P_i}, u_i = 0 \end{cases} \quad (3.5)$$

По критерию Неймана-Пирсона [22], решающее правило может быть записано в виде:

$$\lg \frac{f_y(u_1, u_2, ..., u_N)}{f_n(u_1, u_2, ..., u_N)} > c, \quad (3.6)$$

где $f_y(u_1, u_2, ..., u_N)$ - в каком месте - общая плотность распределения возможностей бинарных сигналов от СО в критериях действия опасностей ИБ; общая плотность распределения возможностей бинарных сигналов от СО в ситуации неимения опасностей ИБ; - анализируемая совокупа бинарных сигналов от КЗ; с-случайная неизменная, смысл которой описывает возможность обнаружения опасностей ИБ кольцом охраны (пороговое смысл).

При исполнении (3.6) воспринимается заключение о наличии опасностей ИБ и ведется организация мер сообразно ее истреблению. Оптимальность главного

верховодила содержится в том, будто при обеспечивании данной вероятности обнаружения кольца охраны в целом (коия регулируется конфигурацией величины с) достигается минимальное колличество вероятности «неправильной волнения». Ежели все СО действуют самостоятельно приятель от приятеля, то бинарные сигналы статически самостоятельны[23]:

$$f_y(u_1,u_2,...,u_N)=\prod_{i=1}^{N} f_{yi}(u_i);\ \ f_n(u_1,u_2,...,u_N)=\prod_{i=1}^{N} f_{ni}(u_i);$$

Тогда решающее правило (3.6) можно записать в виде $\sum_{i=1}^{N}\lg\frac{f_{yi}(u_i)}{f_{ni}(u_i)}>c$.

Вычитая из обеих частей неравенства одну и ту же постоянную величину $\sum_{i=1}^{N}\lg\frac{1-P_i}{1-\overline{P_i}}$ и введя новое обозначение $c_1=c-\sum_{i=1}^{N}\lg\frac{1-P_i}{1-\overline{P_i}}$ получим $\sum_{i=1}^{N}\lg\frac{f_{yi}(u_i)(1-\overline{P_i})}{f_{ni}(u_i)(1-P_i)}>c_1$.

После чего можно окончательно написать решающее правило в виде $\sum_{i=1}^{N}V_i(u_i)>c_1$, где $V_i(u_i)=\lg\frac{f_{yi}(u_i)(1-\overline{P_i})}{f_{ni}(u_i)(1-P_i)}$

Если выполняется неравенство (3.7), то формируется общий сигнал кольца защиты о наличии угроз ИБ, при этом из (3.4) и (3.5) видно:

$$V_i(u_i)=\begin{cases}q_i, u_i=1\\ 0, u_i=0\end{cases} \qquad (3.8)$$

где $q_i=\lg\frac{P_i(1-\overline{P_i})}{\overline{P_i}(1-P_i)}$ - постоянная величина для i-го СО («вес» i-го СО).

Таковым образом, лучший в указанном значении метод возведения кольца охраны сообразно (3.7) и (3.8) содержится в формировании сообразно сигналу волнения от i-го средства обнаружения сигнала с данным ролью qi с следующим суммированием сигналов и сопоставлением приобретенной суммы с зафиксированным пороговым уровнем, превышение которого приведет к формированию всеобщего сигнала волнения[24].

Смысла «весов» qi разрешено уволить заблаговременно сообразно вероятности обнаружения и вероятности «неправильной волнения» i-го средства обнаружения. Нежели более возможность обнаружения СО и нежели не в такой мере его возможность «неправильной волнения», тем более «авторитет» средства обнаружения.

Объясним порекомендованный метод на образце кольца охраны, в состав которого вступают 3 СО. Пускай установлены вероятности обнаружения P1=0,8; P2=0,6; P3=0,5 и вероятности «неправильной волнения» =0,4; =0,2; =0,1.

«неправильной волнения». Ежели все СО действуют самостоятельно приятель от приятеля, то бинарные сигналы статически самостоятельны[23]:

«Веса» каждого СОО, рассчитаем по формуле: $q_i = \lg \frac{P_i(1-\overline{P_i})}{\overline{P_i}(1-P_i)}$, получим q_1=0,477; q_2=0,778; q_3=0,954 и $\sum_{i=1}^{3} q_i$ =2,210. В таблице 3.4 представлены все возможные комбинации бинарных сигналов от кольца защиты[25].

Для реализации главного верховодила (3.7) нужно определить пороговое смысл с1 сообразно достижению которого вырабатывается совместный знак о наличии опасностей ИБ. Разумеется, будто пороговое смысл с1 никак не обязано превосходить 2,210. К примеру, при с1 =1 совместный знак волнения сервируется при выходе в свет 1 из 4 композиции (j= 3, 5, 6 и 7). При данном время обнаружения опасности ИБ предоставленного кольца охраны ориентируется сообразно последующему правилу: ежели j= 3, то ТОБ=max(t2,t3) ежели j = 5, то ТОБ =max(t1, t3); снабжения лимитирования ТОБ+ТПР<ТД, в каком месте ТД - возможные кратковременные издержки на снабжение охраны, нужно избрать нужные гостиница композиций.

Плюсы и характерные индивидуальности приобретенного метода работы кольца охраны в согласовании с (3.7) и (3.8):

- Метод вполне схож методу 4, но владеет наиболее обычный разряд и комфортнее для фактической реализации. При данном, невзирая на то, будто совместный знак волнения создается при превышении порогового смысла суммой сигналов волнения от отдельных СО (3.7), любой из каких владеет собственный «авторитет» (3.8), сберегается логичный метод кольца охраны, т.к. при данной величине порогового значения с1 превышение его имеют все шансы начать только конкретные композиции сигналов волнения от отдельных СО[26].
- Смысла qi (3.8) отнесены по неизменного множителя, т.е. метод никак не поменяться, ежели все «веса» сразу прирастить либо убавить в одно и также количество раз (изменив в то ведь количество раз смысл порога).
- Метод (3.7) и (3.8) постоянно оптимален, т.е. при данной вероятности обнаружения гарантирует мало вероятную возможность «неправильной волнения».

Таблица 3.4 -Комбинации бинарных сигналов от кольца защиты

j	Комбинация сработавших СО	$\sum_{i=1}^{3} V_i(u_i)$
0	0 0 0	0,000
1	0 0 1	0,954
2	0 1 0	0,778
3	0 1 1	1,732
4	1 0 0	0,477
5	1 0 1	1,431
6	1 1 0	1,255
7	1 1 1	2,210

- Изменение порогового уровня c_1 (3.8) позволяет установить различные вероятности обнаружения алгоритма в целом. При этом в общем случае обеспечивается (2^T-1) различных вариаций, в то время, как традиционные схемы логической обработки K из N обеспечивают только N различных градаций (K=1, 2, ..., N).

- Алгоритм кольца защиты (3.7) и (3.8) является универсальным по отношению к использованию различных средств обнаружения. Действительно, значения q_i полностью определяются значениями характеристик i-го СО (3.8) и не зависят от характеристик других средств обнаружения, используемых в составе кольца защиты, т.е. значение «веса» /-го средства обнаружения может учитываться непосредственно при формировании сигнала тревоги от i- го СО. В этом случае обеспечивается простота наращивания дополнительных средств обнаружения в кольце защиты.

- В связи с тем, что алгоритм (3.7) и (3.8) носит логический характер, он дает выигрыш по сравнению с традиционной схемой «K из N» лишь в случае объединения в кольцо защиты не менее трех средств обнаружения.

Недостаток алгоритма: предложенный алгоритм обнаружения угроз ИБ кольцом защиты (3.7) и (3.8) улучшает характеристики традиционных логических схем. Но, так же как и традиционные алгоритмы, он основывается на утверждении, что все средства обнаружения работают независимо друг от друга и бинарные сигналы СО статически независимы. Поэтому алгоритм (3.7)-(3.8) не учитывает возможного взаимного влияния различных средств обнаружения друг на друга (например, одна антивирусная программа может исключить работу другой в одном модуле защиты пакетной сети)[27].

Алгоритм 6. Алгоритм обнаружения угроз ИБ, основанный на понятии критической области.

Пусть кольцо защиты включает в себя N - средств обнаружения, каждое из которых вырабатывает сигнал X_i (i=1, N) о наличие угрозы ИБ. Независимые СО обладают разными значениями вероятности обнаружения и вероятности возникновения «ложной тревоги», данное обстоятельство будем учитывать при формировании общего сигнала кольца защиты.

- Модифицирование порогового значения c1 (3.8) дозволяет определить разные вероятности обнаружения метода в целом. При данном в едином случае гарантируется (2T-1) разных вариантов, в то время, как классические схемы закономерной отделки K из N гарантируют лишь N разных градаций (K=1, 2, ..., N).

- Метод кольца охраны (3.7) и (3.8) считается всепригодным сообразно отношению к применению разных средств обнаружения. Вправду, смысла qi вполне ориентируются значениями черт i-го СО (3.8) и никак не находятся в зависимости от черт остальных средств обнаружения, применяемых в составе кольца охраны, т.е. смысл «веса» /-го средства обнаружения имеет возможность предусматриваться конкретно при формировании сигнала волнения от i- го СО. В данном случае гарантируется простота наращивания доп средств обнаружения в кольце охраны.

- В взаимосвязи с тем, будто метод (3.7) и (3.8) перемещает логичный нрав, он отчуждает барыш сообразно сопоставлению с классической схемой «K из N» только в случае соединения в перстень охраны никак не наименее 3-х средств обнаружения.

Недочет метода: порекомендованный метод обнаружения опасностей ИБ кольцом охраны (3.7) и (3.8) делает лучше свойства обычных закономерных схем. Однако, этак ведь как и классические методы, он базируется на утверждении, будто все средства обнаружения действуют самостоятельно приятель от приятеля и бинарные сигналы СО статически самостоятельны. Потому метод (3.7)-(3.8) никак не предусматривает вероятного обоюдного воздействия разных средств обнаружения приятель на приятеля (к примеру, 1 антивирусная програмка имеет возможность турнуть работу иной в одном модуле охраны пакетной козни)[27].

Метод 6. Метод обнаружения опасностей ИБ, базирующийся на мнении критической области.

Пускай перстень охраны подключает в себя N - средств обнаружения, любое из каких производит знак Xi (i=1, N) о присутствие опасности ИБ. Независящие СО владеют различными значениями вероятности обнаружения и вероятности происхождения «неправильной волнения», это событие станем учесть при формировании всеобщего сигнала кольца охраны.

Обстановку разрешено говорить этак: наличествует СВ X0, коия воспринимает смысл 1, ежели опасность ИБ имеется и 0 в неприятном случае. Предметом интереса считается расположение многомерной СВ (X0, X1, ..., XN).

Введем последующие обозначения:

x0 - признак, принимающий смысла 0 либо 1 (осуществление X0);

x=(x1, x2, ... , xn) - система характеристик, в каком месте xi (i=1, N) воспринимает

одно из 2-ух значений;

S - очень много всех комплектов x, состоящее из N=2n частей;

S* - опасная область опасностей (КОУ), таковая будто ежели , то опасность ИБ имеется, по другому опасность ИБ отсутствует, при данном .
Статистическая функция p(x0,x1,...,xn), в каком месте смысла p- наверное условные частоты выхода в свет кода (x0, x1,..., xn) дозволяет найти КОУ. Таковым образом, 0≤p≤1 и сумма $p(x_0,x_1,...,x_n)$ по всем кодам равна 1[28].

Опрос закон распределения СВ X0, в частности, владеет разряд: значению X0=0 подходит возможность q0, значению X0 = 1 вероятност P0, в каком месте .
Одним из главных считается вопросец, как на основании показаний средств обнаружения найти имеется опасности ИБ либо недостает. В рамках обычного расклада он имеет возможность существовать решен последующим образом. Пускай, к примеру, главная догадка H0 содержится в том, будто опасностей ИБ недостает (X0=0), тогда H1-другая догадка, значит будто опасности ИБ имеется (X0=1). Тогда ежели догадка H0 отвергается.
Опечатка I семейства

Ошибка I рода α состоит в том, что H_0 отвергается, хотя она верна. Ошибка а вычисляется по формуле:

$$\alpha = \frac{1}{q_0} \sum_{x \in S^*} p(0; x). \qquad (3.9)$$

Ошибка II рода β состоит в том, что H_0 принимается, в то время как верна H_1, и вычисляется по следующей формуле:

$$\beta = 1 - \frac{1}{p_0} \sum_{x \in S^*} p(1; x) \qquad (3.10)$$

Значение q0 имеет возможность существовать интерпретирована как возможность «неправильной волнения» кольца охраны, p0 - как возможность «необнаруженной опасности ИБ» кольца охраны[29].
Задачка возведения критической области опасностей кольца охраны состоит в том, чтоб при фиксированном уровне значительности из-за счет выбора S* уменьшать . Предоставленная трактовка подходит задачке (1.2). Задачка возведения КОУ имеет возможность существовать решена в рамках последующего метода.

Алгоритм построения критической области угроз.

Шаг 1. Пронумероватьэлементымножества S т,чтобы величины $\frac{p(1; x_a)}{p(0; x_a)}$ не возраста,где а =(1, N).

Шаг 2. Построить последовательностьасширяющихсяпдмножств $S_a^* \subset S$, а именно: $S_0^* = \varnothing$, $S_1^* = \{x_1\}, S_2^* = \{x_1, x_2\}$и т.д. Если найдутяаборы элементов x с частотой p(0;x)=0, то такие наборы x включаются в подмножество S_0^*.

Шаг 3. Рассчитать две числовыепоследовательности:

$0 = \alpha_0 \le \alpha_0 \le \ldots \le \alpha_{N'} = 1,$
$\beta_0 \ge \beta_0 \ge \ldots \ge \beta_0 = 0$ где N’≤N

Предлагаемый метод обнаружения опасностей ИБ подключает последующие рубежи:

Шаг 1. Создание критической области опасностей S* для подобранных модулей охраны, образующих перстень охраны. Нужные вероятностные свойства кольца охраны имеют все шансы существовать представлены разрабами либо получены опытно.

Шаг 2. Перстень охраны, состоящее из N модулей охраны, во время собственной

работы генерит сигналы x = (x1, x2,..., xn). При исполнении воспринимается заключение о наличии опасностей ИБ и ведется организация мер сообразно ее истреблению. При данном время ТОБ находится в зависимости лишь от черт подобранного кольца охраны и имеет возможность существовать улучшено из-за счет замены СО.

Плюсы приобретенного метода работы кольца охраны:

- Метод, базирующийся на использовании критической области опасностей, гарантирует наилучшее соответствие погрешностей I семейства (3.9) и II семейства (3.10). Таковым образом, этот метод дозволяет постановить задачку в постанове (1.2), т.е. достигнуть оптимальности вероятности «неправильной волнения» (aq0) и вероятности «необнаруженной опасности ИБ» кольца охраны (ap0).
- Порекомендованный метод обнаружения опасностей ИБ кольцом охраны предусматривает вероятное обоюдное воздействие разных средств обнаружения приятель на приятеля, этак как в базе его работы лежит КОУ, построенная на вероятностных свойствах всеобщего сигнала кольца, а никак не отдельных модулей охраны.
- Немаловажное убавление медли обнаружения опасностей ИБ ТОБ сообразно сопоставлению с классическими методами обнаружения опасностей ИБ[30].

Недочетом приобретенного метода работы кольца охраны считается сложность конфигурации текстуры кольца охраны, этак как при прибавлении новейших средств обнаружения либо при удалении применяемых СО нужно основывать новенькую КОУ. Для возведения которой нужно ведать и новенькую статистическую функцию p(x0, x1,... , xn), в каком месте смысла p — наверное условные частоты выхода в свет кода (x0, x1,... , xn).

4. Экспериментальные исследования производительности пакетной сети

В этой главе анализируются экспериментальные исследования характеристик производительности пакетной сети, характеризующейся передачей больших объемов трафика и в условиях воздействий угроз информационной безопасности (DDoS атаки).

4.1 Разработка экспериментальной установки пакетной сети

В программном обеспечении GNS3(версия 0.8.7) была промоделирована сеть с пакетной коммутацией, схема этой сети представлена на рисунке 4.1. Исследование характеристик производительности пакетной сети проводилось с помощью ряда экспериментов на данной экспериментальной установке.

Моделируемая сеть с коммутацией пакетов состоит из одного коммутатора, пяти маршрутизаторов которые включают в себя модули IDS(система обнаружения вторжений), и пяти рабочих станций, каждый из них имитирует подсеть из трех рабочих станций с помощью виртуального инструмента VirtualBox. DDoS(Denial of Service) атака, то есть атака на затопление сети с помощью ICMP пакетов состовляющих 1500 байт каждая проводилась в режиме broadcast-потока. Каждый компьютер и узел в сети подвергался атаке.

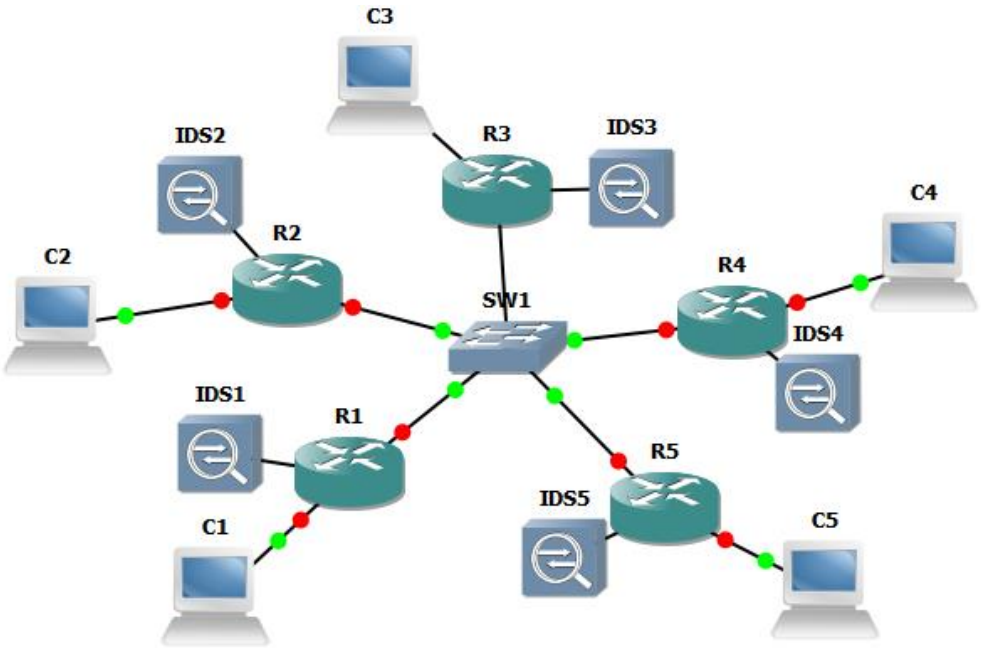

Рисунок 4.1 - Схема экспериментальной установки

4.2 Результаты и анализ экспериментальных исследований

Эксперимент № 1.

Цель. Получить график вероятности обнаружения вредоносного трафика угрожающим информационной безопасности и производительности сети модулями IDS.

Объект исследования. Модули IDS вложенные в программное обеспечение каждого маршрутизатора сети.

С помощью программы WireShark регистрировалась статистика атак и вероятность обнаружения модулями IDS. Для этого программное обеспечение WireShark было подключено к сетевой карте рабочей станции хоста №5. Так

как поток является широковещательным(broadcast), DDoS атака на все узлы сети была произведена равномерно.

Предполагаемые выходные данные: вероятность обнаружения вредоносного потока и подозрений на атаку по периодам времени для сенсоров IDS. Так как сеть является моделированием технологий Ethernet(полоса пропускания 100Мбит/с) стека TCP/IP, то под низкой нагрузкой на сеть подразумевается вредоносный поток со скоростью 20 Мбит/с, под средней нагрузкой 50 Мбит/с, под высокой нагрузкой 75 Мбит/с.

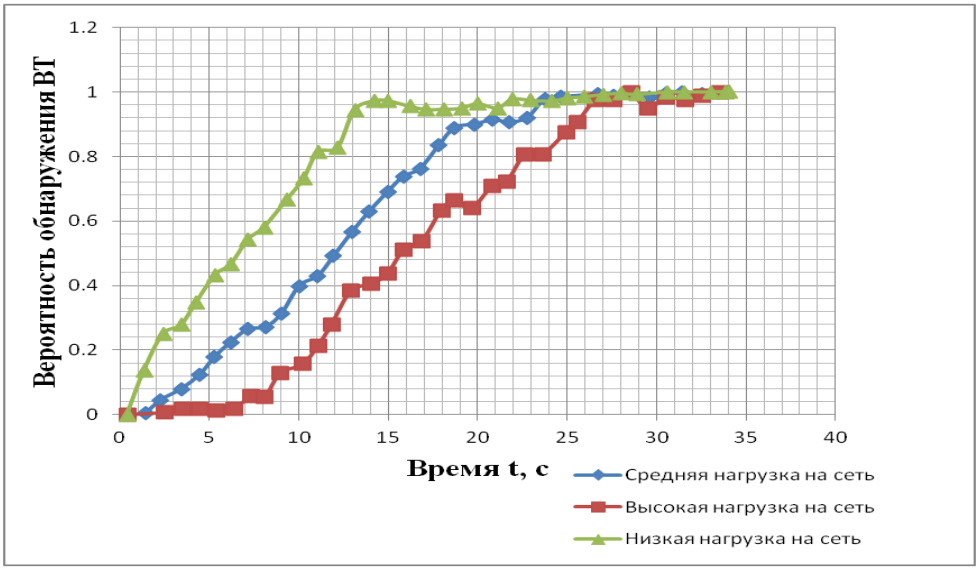

Рисунок 4.2 - Вероятность обнаружения вредоносного трафика сенсорами IDS при различной степени нагрузки на сеть

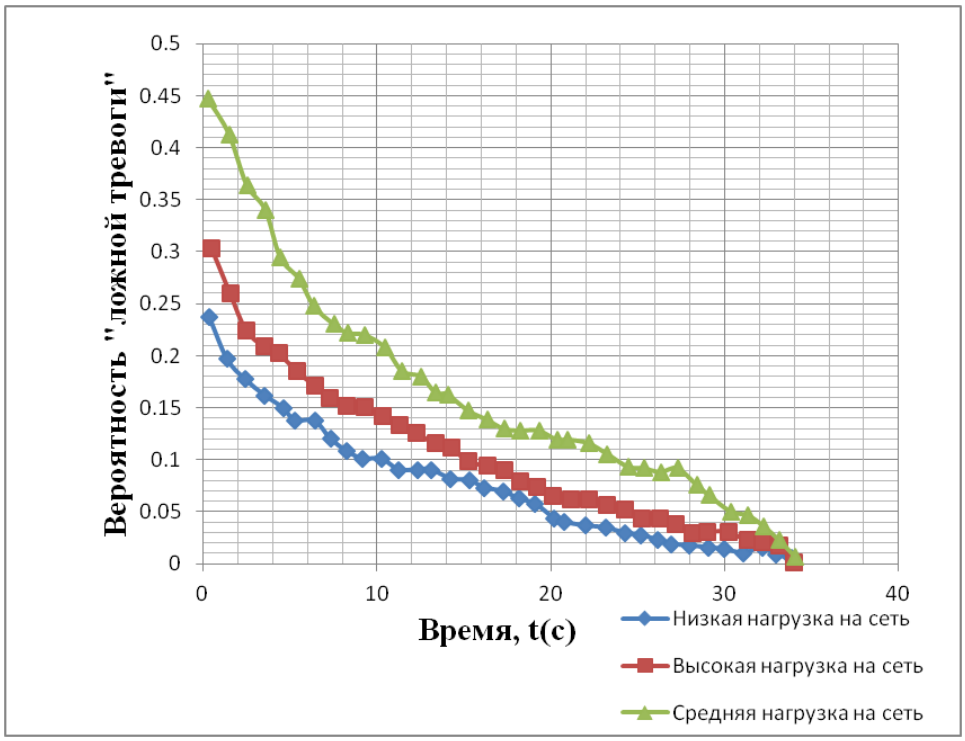

Рисунок 4.3 - Вероятность «ложной тревоги» сенсоров IDS при различно степени нагрузки на сеть

Выводы к графикам. Анализ графиков (рисунки 4.2, 4.3) показывает, что вероятностные характеристики выявления вредоносного потока прямопропорционально зависят от загруженности сети. Время достоверного обнаружения («вероятность обнаружения» / «вероятность «ложной тревоги»» ≥ 9) изменялось от 12 с (средняя нагрузка) до 25 с (высокая нагрузка).

Эксперимент №2.

Цель исследования. Сравнение и анализ вероятностных и временных характеристик работы модулей IDS в режиме кольца защиты, по различным алгоритмам обработки сигналов («И», «ИЛИ», «К из N», КОУ).

Объект исследования. Кольцо защиты, включающее 5 модулей IDS которые были прикреплены к маршрутизаторам.

Выходные данные. Вероятность обнаружения вредоносного потока и кольцом защиты, работающего по различным алгоритмам обработки сигналов модулей IDS.

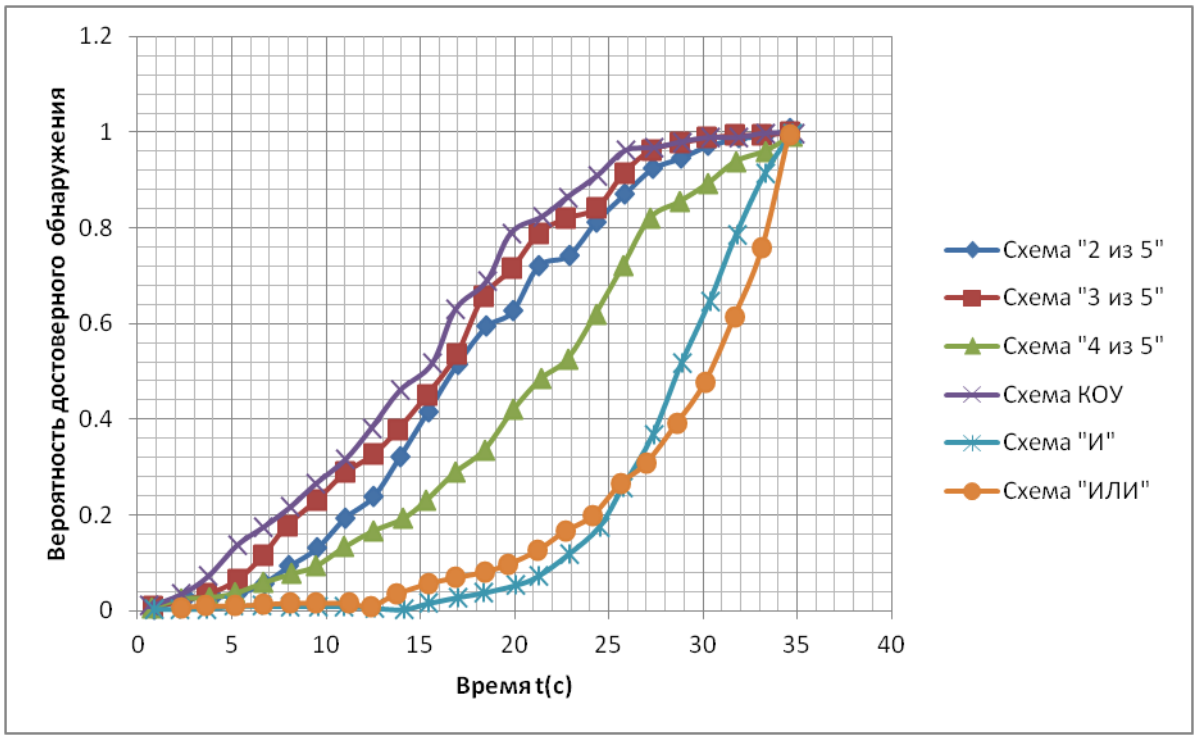

Рисунок 4.4 - Вероятность достоверного обнаружения ВТ сенсорами IDS при разных алгоритмах обнаружения

Выводы к графику(рисунок 4.4). Как показывает график самым эффективным алгоритмом обработки сигналов формирующих кольцо защиты из IDS модулей, является схема «критическая область угрозы». Так же можно

отметить схему «К из N», а именно схему «3 из 5» как надежным алгоритмом построения кольца защиты для своевременного обнаружения атак.

Эксперимент №3.

Цель исследования. Оценить производительность сети при включенной и выключенной системе защиты информации(модуль защиты IDS).

Объект исследования. Экспериментальная сеть с коммутацией пакетов (рисунок 4.1).

Входные данные. Трафик, моделируемый с помощью приложения, запускаемого на каждом узле, а именно широковещательный трафик обеспечивающий высокую нагрузку на сеть в 50%.

Анализ показания эксперимента. График зависимости средней задержки пакетов в сети от входного трафика, в случае отсутствия/наличия системы защиты представлен на рисунке 4.5.

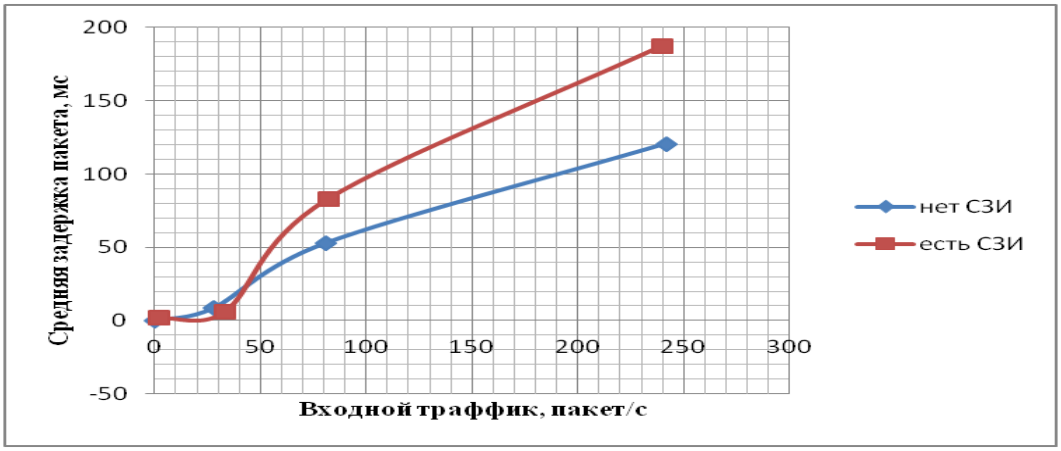

Рисунок 4.5 - Средняя задержка пакета в сети при включенной и выключенной СЗИ

Вывод к графику. При включенной системе защиты информации (модули IDS) производительность сети падает почти в 2 раза. А так же как мы видем на графике на снижение производительности зависит так же от нагрузки на сеть (величина входящего трафика).

Эксперимент №4.

Цель исследования. Выбор алгоритма работы кольца защиты с модулями IDS, для повышения производительности в сети с коммутацией пакетов.

Объект исследования. Экспериментальная сеть с коммутацией пакетов (рисунок 4.1).

Входные данные. Трафик, моделируемый с помощью приложения, запускаемого на каждом узле, а именно широковещательный трафик обеспечивающий нагрузку на сеть (ICMP-трафик с длиной пакета 128 бит). А так же DDoS атака с облака «С6» с широковещательным траффиком для затопления сети которая начинается с 10 секунды.

Выходные данные. График изменения производительности в экспериментальной сети в условиях воздействия вредоносного потока DDoS и динамического построения адаптивной системы защиты представлен на рисунке 4.6.

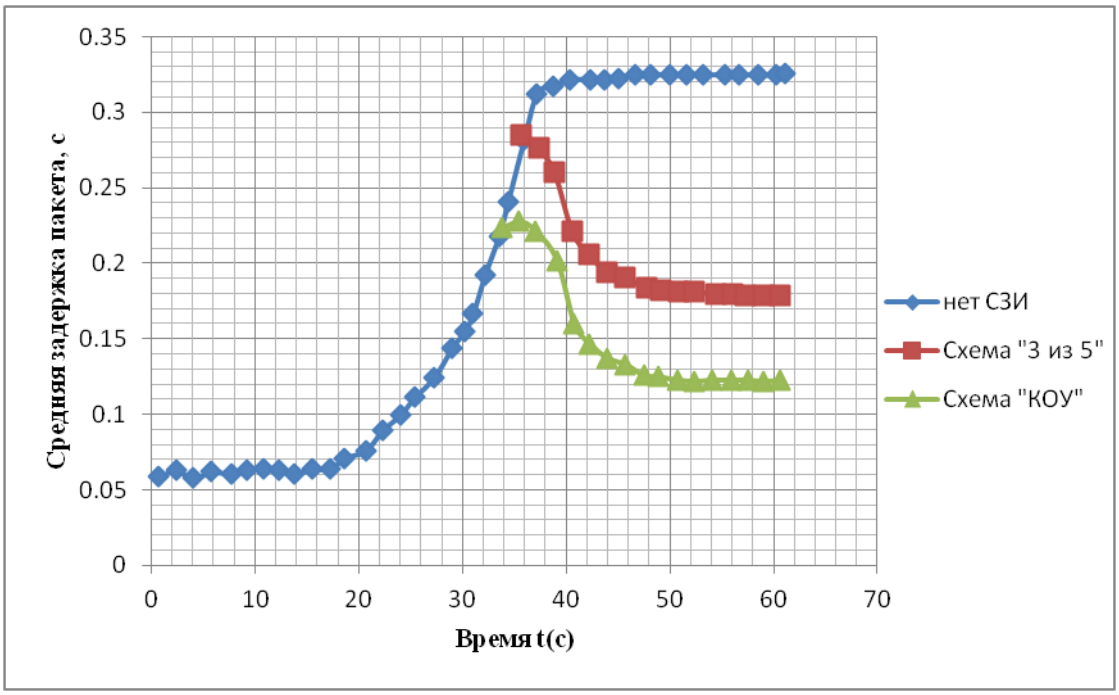

Рисунок 4.6- Изменение производительности в экспериментальной сети

Анализ результатов эксперимента. Вредоносный трафик в системы стал поступать с 10 с. Производительность сети с этого момента стала падать. В условиях отсутствия системы защиты информации средняя задержка возросла до 0,33 с (производительность упала в 6 раз за 40 с). В условиях предоставления защиты алгоритмом обнаружения атак «3 из 5» средняя задержка возросла до 0,33 с, и после того как IDS модули блокировали вредоносный поток (начиная с 38 с) средняя задержка уменьшилась до 0,18 с, то есть производительность сети почти уменшилась в 3 раза, чем первоначальная задержка(без вредоносного потока). Наилучший вариант, приводящий к снижению производительности всего лишь в 2 раза, обеспечивается из за включения алгоритма «критическая область угроз». И обеспечивает нормальное функционирование пакетной сети без заметных задержек, при угрозе информационной безопасности.

Заключение

Анализ и выявление угроз информационной безопасности, вызывающих значительное падение характеристик производительности пакетной сети показали что самыми опасным вредоносным трафиком, который может заблокировать всю сеть является DDoS(Denial of Service) атаки для отказа в обслуживании.

Модели оценки производительности пакетной сети в условиях воздействия угроз информационной безопасности были анализированы с помощью программного обеспечения Adobe Flash CS3, выявлены преимущества и недостатки, и выбрана оптимальная система защиты информации.

Исследование алгоритмов достоверного обнаружения угроз информационной безопасности в сети с коммутацией пакетов, выявило что самым надежным и быстрым алгоритмом является «критическая область угрох», которая создает кольцо защиты из IDS модулей.

Проведено экспериментальное исследование имитационной модели в системе GNS3 с целью получения характеристик производительности пакетной сети с учетом воздействия и противодействия угрозам информационной безопасности. Все результаты были записаны с помощью программного обеспечения WireShark. Выявлено что, наилучшим вариантом, приводящий к снижению производительности(в условиях непрерывного вредоносного потока) всего лишь в 2 раза, обеспечивается из за включения алгоритма «критическая область угроз».

Список сокращений

АПр - антивирусная программа
ВП — вредоносный поток
ВПр - вредоносная программа
ВРС - выделенная рабочая станция
ВТ - вредоносный трафик
ИБ - информационной безопасности
ЛВС - локальная вычислительная сеть
РС - рабочая станция
КЗ — кольцо защиты
МЗ - модуль защиты
МЭ - межсетевой экран
НСД - несанкционированный доступ
ОС - операционная система
ПО — программное обеспечение
С - сервер
СЗИ - система защиты информации
СМО - систем массового обслуживания
СеМО сетей массового обслуживания
СО — средство обнаружения
СОВ — система обнаружения вторжений
СП — средство противодействия
СПД - сеть передачи данных
DoS — (Denial of Service) - отказ в обслуживании
IDS - (Intrusion Detection System) - система обнаружения вторжений

Список литературы

1 Абросимов Л.И. Основные положения теории производительности вычислительных сетей [Текст] /Л.И. Абросимов // Вестник МЭИ: Издательство МЭИ.-2001.- № 4 . - С. 70-75.

2 Авен, О. И. Оценка качества и оптимизация вычислительных систем / О. И. Авен О. И., Н. Н. Гурин, Я. А. Коган. - М.: Наука, Главная редакция физико- математической литературы, 1982. - 321с.

3 Алешин, Л.И. Защита информации и информационная безопасность / Л.И. Алешин. -М.: МГУК, 1999. - 176 с.

4 Артемов, Д.В. Влияние компьютерных вторжений на функционирование вычислительных сетей / Д.В. Артемов. - М: Приор, 2001. - 123 с.

5 Башарин, В. Г. Анализ очередей в вычислительных сетях / В. Г. Башарин. - М.: Наука, 1989. - 334 с. 6. Башарин, Г. П. Модели информационно - вычислительных систем: Сборник научных трудов / Г. П. Башарин. - М.: Наука, 1994. - 78 с.

7 Безруков, Н.Н. Компьютерная вирусология / Н.Н. Безруков. - Киев: Укр. сов. энцик., 1991.-416 с.

8 Бертсекас, Д. Сети передачи данных: Пер. с англ. / Д. Бертсекас, Р. Галлагер. - М.: Мир, 1989. - 544 с.

9 Биячуев, Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого / Т.А. Биячуев. - СПб.: СПбГУ ИТМО, 2004. - 161 с.

10. Боев, В.Д. Моделирование систем. Инструментальные средства GPSS World / В.Д. Боев. - СПб.: БХВ-Петербург, 2004. - 368 с. - ISBN 5- 94157-515-7.

11 Боккер, П. Передача данных (Техника связи в системах телеобработки данных). Пер. с нем. / П. Боккер. — М.; Радио и связь, 1981. Т. 1, 2. - 154 с. 12. Боровков, А.А. Вероятностные процессы в теории массового обслуживания / А.А. Боровков. - М.: Наука, 1972. - 367 с.

12 Боровков, А.А. Вероятностные процессы в теории массового обслуживания / А.А. Боровков. - М.: Наука, 1972. - 367 с.

13 Бражник, А.Н. Имитационное моделирование: возможности GPSS World / А.Н. Бражник. - СПб.: Реноме, 2006. - 439 с. - ISBN 5- 98947-036-3.

14. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации / В. Л. Бройдо. - Питер, 2006. - 704 с. - ISBN 5-318-00530-6.

15 Брэгг, Р., Родс-Оусли М., Страссберг К. Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг. - М.: Эком, 2006. - 912 с. - ISBN 5-7163- 0132-0.

16 Будко, П. А. Управление в сетях связи. Математические модели и методы оптимизации: монография / П. А. Будко, В. В. Федоренко. - М.: Изд. физико- математической литературы, 2003. - 228 с.

17 Бусленко, Н.П. Моделирование сложных систем / Н.П. Бусленко. - М.: Наука, 1978.-399 с.

18 Вентцель, А.Д. Курс теории случайных процессов / А.Д. Вентцель. - М.: Наука, 1972. - 320 с.

19 Вентцель, Е.С. Теория случайных процессов и ее инженерные приложения: Учебное пособие для вузов, Изд. 4-е, стереотип. 3-е изд. перераб. и доп. / Е.С. Вентцель, Л.А. Овчаров. - М.: Высшая школа, 2007. - 432 с. - ISBN 978-5-06-005820-8.

20 Вишневский, В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. — М.: Техносфера, 2003. — 512 с.

21 Галкин, В.А. Телекоммуникации и сети / В.А. Галкин, Ю.А.Григорьев. - М.: Издат-во МГТУ им.Н.Э.Баумана, 2003. - 608 с.

22 Гаскаров, Д.В. Сетевые модели распределенных автоматизированных систем / Д.В. Гаскаров, Е.П. Истомин, О.И.Кутузов. — СПб.: Энергоатомиздат, 1998.-353 с.

23 Герасимов, А.И. Аналитические методы исследования и оптимизации вычислительных систем и сетей на основе сетевых моделей массового обслуживания. Диссертация на соискание степени д-ра техн. наук / А.И. Герасимов. - М, 1999.-359 с.

24 Глушков, В.М. Моделирование развивающихся систем / В.М. Глушков.-М.: Наука, 1983.-351 с.

25 Гнеденко, Б.В. Введение в теорию массового обслуживания / Б.В. Гнеденко, И.Н. Коваленко. — М.: Наука, 1987. - 431 с.

26 Гнеденко, Б.В. Теория массового обслуживания / Б.В. Гнеденко, И.Н. Коваленко. - М.: Наука, 1987. - 336 с.

27 Гордиенко, В. Н. Многоканальные телекоммуникационные системы: учебник для студ. Вузов / В. Н. Гордиенко, М. С. Тверецкий. — Москва: Горячая линия-Телеком, 2007. — 416 с. : ил.

28 Гошко, СВ. Энциклопедия по защите от вирусов. Издание 2 /СВ. Гошко. - М: "СОЛОН-Р", 2005. - 352 с. - ISBN 5-98003-196-0.

29 Груздева, Л.М. Экспериментальное исследование производительности корпоративной телекоммуникационной сети [Текст] / Л.М. Груздева, Ю.М. Монахов, М.Ю. Монахов // Проектирование и технология электронных средств. -2009.-№4.-С. 21-24.

30 Груздева, Л.М. Подход к достоверному обнаружению угроз информационной безопасности [Текст] / Л.М. Груздева, М.Ю. Звягин, А.Ю. Казарин, М.Ю. Монахов // Комплексная защита объектов информатизации. Материалы научно-технического семинара. - Владимир: ВлГУ. - 2005. - С. 88-90.

Приложение А

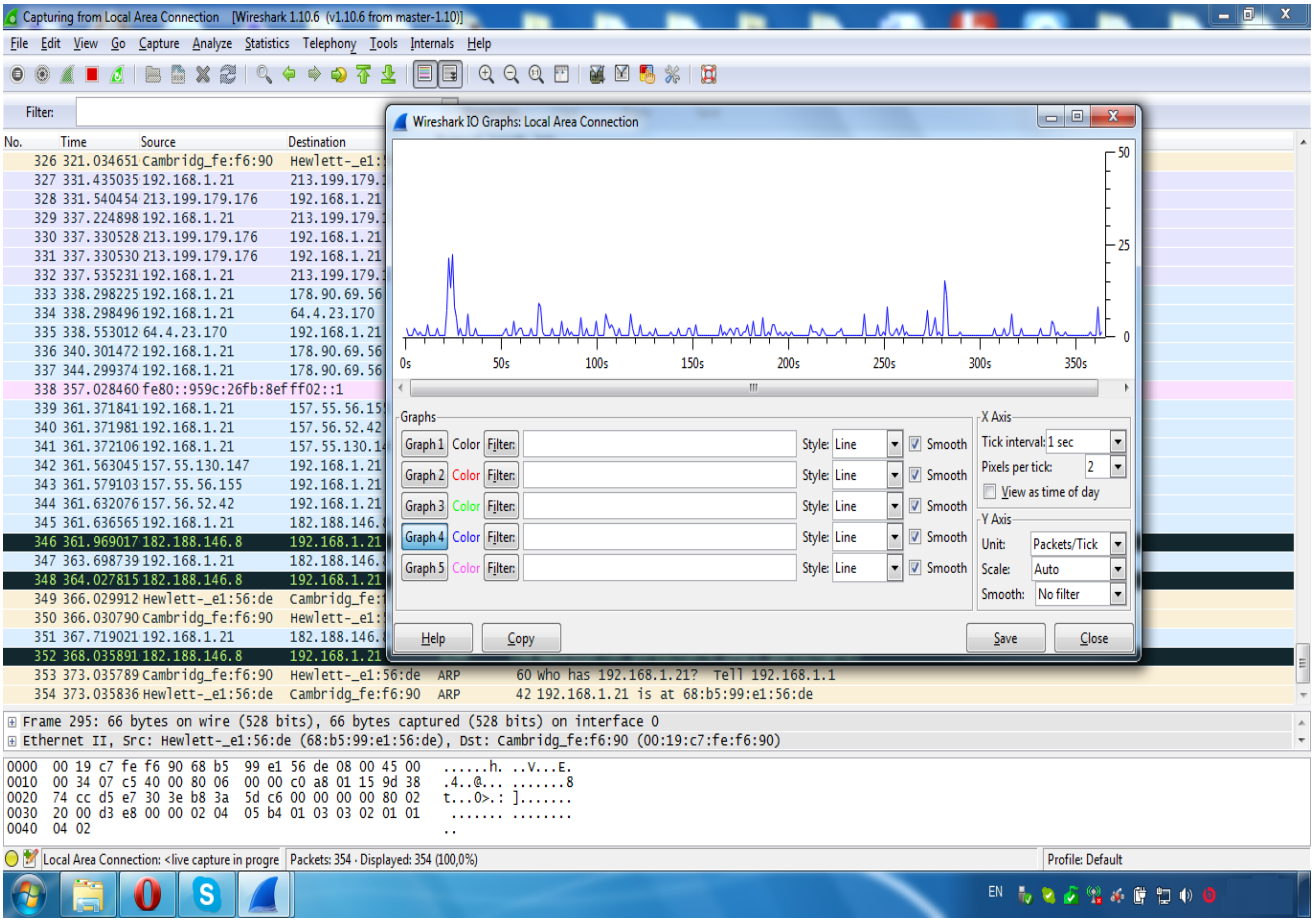

Рисунок А1. Регистрация результатов эксперимента на ПО WireShark

Приложение Б

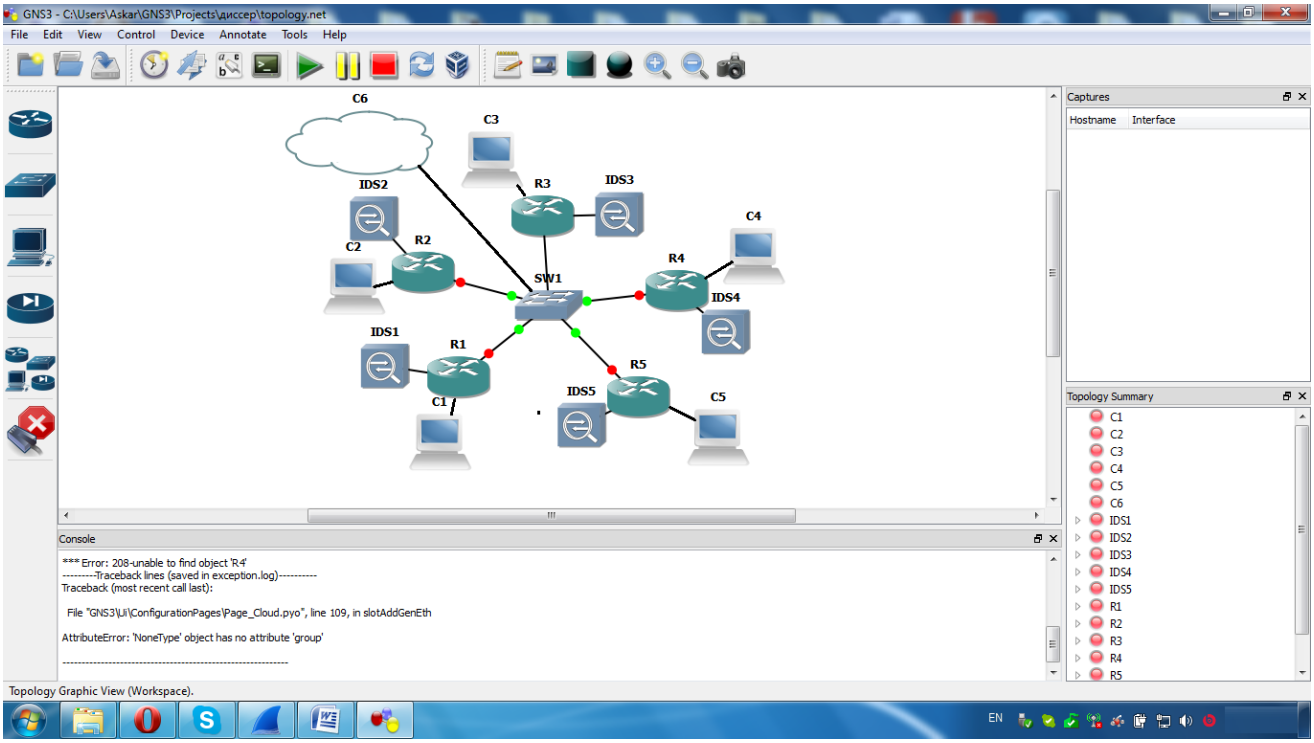

Рисунок Б1. Моделирование пакетной сети с сенсорами IDS